PROPOSITION DE CADRE TECHNO-NORMATIF DE COLLECTE ET TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL DANS LA GESTION ET LA SORTIE DE CRISE COVID-19

Pour un encadrement démocratique des usages

https://tfc19.tech/

Sous la direction scientifique de J.J. ATTIA et C. LEQUESNE ROTH

Aves les contributions de J.J. ATTIA, A. BAYLE, A. EL BROUDI , J. CAFFIN, J. KELLER, P. LEGROS, C. LEQUESNE-ROTH, C. LEVALLOIS-BARTH, J. MARCEAU, T. VERBIEST[1]

Version 2.0 - 24 avril 2020

[1] Nous tenons à remercier, pour leur relecture et précieux conseils : G. BLOT, S. LAMOUDI, M. QUINIOU et S. VILLATA.

Dans la lutte menée par les États et les institutions de santé contre la pandémie Covid-19, les outils numériques font désormais partie intégrante des solutions de prévention et de soins envisagées, au même titre que les diagnostics et traitements médicaux conventionnels. Et c'est une première dans l'histoire à la fois de la médecine et de la gestion des crises sanitaires.

C'est ainsi que des « technologies et outils numériques de localisation/suivi des personnes infectées » sont actuellement en développement et ne manquent pas de susciter des questions, craintes et prises de position, non seulement quant à leur pertinence et fiabilité, mais encore quant aux risques qu'ils sont susceptibles de représenter tant pour les libertés individuelles que pour la souveraineté des États membres de l'Union européenne. Les initiatives n'ont pas manqué de se multiplier : applications de traçage décentralisées, de suivi de contacts, de localisation, de verrouillage, de quarantaine individuelle, d'auto-évaluation ou encore d'analyses statistiques[2].

L'un des objectifs poursuivis est de permettre aux personnes contaminées de prévenir ceux et celles avec qui elles ont été en contact pour ralentir la propagation du virus et apporter une réponse idoine (délivrance de tests, anticipation des besoins médicaux, et plus largement, gestion des moyens sanitaires). Un traçage au moyen d'une application mobile, prévenant automatiquement les individus ayant croisé une personne déclarée contaminée, peut faciliter le processus. Ce traçage peut se réaliser soit via la localisation GPS, grâce à laquelle le système identifie les itinéraires des personnes croisées, soit via le protocole de télécommunication Bluetooth, système de pair-à-pair et collectant moins de données à caractère personnel. Cette dernière technique est celle privilégiée dans la plupart des autres États membres de l'Union européenne, ou encore au Japon, car jugée moins intrusive.
Hors Union européenne, le souci de recourir à des technologies de surveillance moins invasives est moins prégnant, et revêt toutes les formes du biocontrôle[3]. Il en est ainsi de l'application AC19 en Iran, des dispositifs de reconnaissance faciale dotés de capteurs thermiques en Russie, en Chine et en Corée du Sud, de la réutilisation des données bancaires, téléphoniques ou celles partagées sur les réseaux sociaux dans les applications de ces mêmes pays ou du recours aux drones. Le risque d'un basculement vers l'autocratie numérique

[2] Pour une recension, voy. Projects using personal data to combat SARS-CoV-2 [en ligne]
[3] Pour le chercheur Yuval Noah Harari, ce choix technologique marque la transition d'un contrôle « sur la peau » à un contrôle « sous la peau », « The world after coronavirus », *Financial Times*, March 20, 2020 [en ligne] https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75

inquiète, et appelle à la plus grande vigilance. Là où la pandémie ne doit reléguer au second plan les libertés individuelles, l'enjeu européen est désormais de créer un système visant à ralentir la propagation du virus via des dispositifs de traçage des individus, décentralisés, sécurisés, mais surtout respectueux de la confidentialité et de la vie privée des citoyens.

Si les initiatives se multiplient à l'échelon national, l'Union Européenne invite les Etats membres à une approche concertée et unifiée au niveau européen[4]. Prenant en compte les réserves du Comité européen de la protection des données (ci-après CEPD) quant à une solution technique unique, elle propose l'élaboration d'un cahier des charges technico-juridique. Ce dernier prévoit une coopération des États parties à une coopération dans la définition des données nécessaires pour répondre aux besoins de recherches épidémiologiques. La réponse à ces besoins présuppose donc un niveau de granularité d'informations nécessaires pour achever la présente crise et prévenir la suivante. Ainsi, les exigences médicales définies dans les prochaines semaines détermineront l'étendue de la collecte de données nécessaires.

C'est dans ce contexte qu'un collectif de data scientists, ingénieurs et juristes, le collectif Task Force Covid 19 (ci-après TFC19), s'est créé. Ce groupe de travail n'a nullement vocation à promouvoir une gouvernance algorithmique. Face aux réalités qui saisissent les démocraties, l'urgence dans laquelle les gouvernements échafaudent des outils numériques de gestion de crise, il apparaît toutefois indispensable d'accompagner la réflexion engagée. L'impériosité de cette démarche est d'autant plus essentielle que :

- Ces outils, même adoptés sous le joug de l'exceptionnalité, poseront les jalons du service numérique de santé de demain ;
- Le débat sur les architectures techniques, éminemment politiques, ne peut être entièrement dévolu aux grands groupes technologiques, au premier rang desquels les GAFAM.

Le collectif TFC19 s'est fixé pour mission de définir un cadre techno-normatif encadrant l'usage de ces technologies numériques dans la lutte contre la pandémie. Ce cadre repose sur dix exigences techno-normatives qui constituent l'horizon démocratique que doit observer tout dispositif de traitement des données à caractère personnel développé dans le cadre de la gestion de crise sanitaire.

[4] Voy. en ce sens, COMMISSION EUROPÉENNE, *Recommendation of 8.4.2020 on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data*, April 8th 2020, C (2020) 2296 final., p.7.[en ligne]. https://ec.europa.eu/info/sites/info/files/recommendation_on_apps_for_contact_tracing_4.pdf

Ces exigences doivent être pensées *a priori*, dès la conception d'un système technique, et intégrées « by design ». Elles sont indispensables au respect du droit de la protection des données et des libertés fondamentales.

La synthèse des principes (I) est suivie de l'étude exhaustive de l'encadrement techno-normatif proposé (II), et des synthèses techniques (III).

SOMMAIRE

I. SYNTHÈSE DES PRINCIPES

1. Tout dispositif algorithmique repose sur une **démarche volontaire**, prévenant et **prohibant tout préjudice ou toute forme de discrimination** à l'encontre des personnes qui refuseraient d'y souscrire.

2. Les finalités de la collecte et des traitements sont **orientées vers la gestion et sortie de crise** ; les données à caractère personnel collectées et exploitées sont restreintes et limitées à cette stricte finalité. Leur collecte devra être minimisée aux seules données nécessaires à la réalisation des objectifs susmentionnés. La pertinence des traitements se fonde à cet effet sur les décisions des autorités publiques, et/ou les recommandations des autorités sanitaires compétentes.

3. Tout dispositif algorithmique est déployé à titre exceptionnel. La loi détermine, en amont de son entrée en application, un **critère d'événement calendaire** de sortie de crise déterminant **la fin du dispositif**.

4. La collecte automatique de données de **géolocalisation est interdite.**

5. Un **profilage** des individus de **type « social »**, étranger aux finalités du traitement, élaboré à partir des données à caractère personnel qui auraient été collectées, est **interdit**, au même titre que toute réutilisation des données à caractère personnel dans un traitement poursuivant une finalité étrangère à la gestion et/ou sortie de crise.

6. Tout dispositif algorithmique est **transparent**, **traçable et auditable** en **libre-accès**.

   Les audits algorithmiques reposent conjointement sur :

   - Des **garanties techniques** assurant la transparence du code, et la traçabilité des données comme des usages, mais également la protection des données à caractère personnel des utilisateurs en cas de compromission du système ;
   - Des **garanties humaines** pour l'usage de chaque outil du dispositif, assurées par des collèges d'évaluation *ad hoc*.

   Ces garanties :

   - Assurent la **conformité** des dispositifs à l'état de droit en général, au respect des finalités identifiées et désignées en particulier ;

- Préviennent et corrigent l'existence ou l'apparition de **biais algorithmiques** ;
- Privilégient la confidentialité et visent à **limiter tout risque d'atteinte à la vie privée** des utilisateurs.

7. Tout dispositif algorithmique offre et garantit une stricte **anonymisation** des données à caractère personnel :
   - Totale ou partielle pendant la crise, notamment avec l'octroi d'identifiants ;
   - Irréversible après la crise.

   Ces techniques doivent être combinées à des dispositifs de chiffrement et de stockage sécurisé des données.

8. Les données sont centralisées sur des serveurs nationaux garantissant la **souveraineté numérique** de l'Etat.

9. La **vente à des tiers** des données à caractère personnel collectées par tout dispositif algorithmique est interdite.

10. Tout dispositif algorithmique garantit **l'égalité devant le service public** ; des **solutions alternatives au numérique** sont proposées.

II. ETUDE

La présente publication formule ci – après :

- Les principes techno-normatifs encadrant la proposition de dispositif ;
- Ses fondements juridiques ;
- Les solutions techniques retenues pour s'y conformer.

Juridiquement, elle se fonde sur :

- Le droit de l'Union Européenne dans son sens le plus large ;
- La déclaration du CEDP du 19 mars 2020 relative au traitement des données à caractère personnel dans le contexte de l'épidémie du Covid-19 ;
- La lettre du CEPD adressée à O. MICOL du 14 avril 2020 ;
- Les lignes directrices du CEPD en date du 21 avril 2020 - *Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak.*
- La recommandation de la Commission 2020/518 sur la constitution d'une boîte à outil commune à l'Union pour l'utilisation de technologie et de donnée afin de combattre et sortir de la crise du Covid-19, spécifiquement aux applications mobiles et à l'utilisation de données de mobilités anonymisées ;
- La boîte à outil commune de l'Union Européenne à destination des Etats Membres, v.1.0, du 15 avril 2020 ;
- Le rapport de l'Agence pour les droits fondamentaux de l'Union Européenne (FRA), *Coronavirus pandemic in the EU, Fundamental rights implication*, Avril 2020.

1. Consentement

Tout dispositif algorithmique repose sur une **démarche volontaire**, prévenant et **prohibant toute forme de discrimination** à l'encontre des personnes qui refuseraient d'y souscrire[5]. Cette démarche volontaire ne soumet pas le responsable au seul fondement licite du consentement[6].

[5] Voy. dans ce sens, CEPD, lettre du 14 avril 2020, *« The enactment of national laws, promoting the voluntary use of the app without any negative consequence for the individuals not using it, could be a legal basis for the use of the apps »*.

[6] Voy. dans ce sens, CEPD, lettre du 14 avril 2020, « *The EDPB notes that the mere fact that the use of the contract tracing takes place on a voluntary basis, does not mean that the processing of personal data by public authorities necessarily be based on the consent* ».

⚖ a. Base légale des dispositifs de traçage : consentement ou intérêt public ?

La question est sensible au regard de ses implications : peut-on imposer un traitement de données à caractère personnel au nom de l'intérêt public, au risque de porter atteinte, de manière disproportionnée, à la vie privée ? Peut-on imposer le développement d'une application sans le consentement des personnes ? La question est d'autant plus prégnante que le RGPD offrirait un fondement juridique à pareille solution[7]. Dans la négative, le consentement peut-il suffire à l'adhésion du plus grand nombre, qui conditionnera l'efficacité du dispositif adopté ?

Les récentes positions institutionnelles, adoptées à l'échelon européen, ne tranche pas le débat. La CEPD appelle les États à privilégier, à titre prioritaire, des modalités d'une collecte de données anonymisées, exclues du champ d'application du RGPD[8] ; la collecte de données à caractère personnel ne doit être envisagée qu'à titre subsidiaire, dans des conditions respectueuses du principe de proportionnalité[9].

Dans l'hypothèse d'un traitement de données à caractère personnel, le CEPD encourage les États membres à recourir aux fondements de l'intérêt public (art. 6,1,d) ou du consentement (art.6,1,a)[10].

Les dispositions de la directive communications électroniques relatives à l'agrégation des données de télécommunication par les opérateurs téléphoniques[11] ne contraignent pas davantage les États membres à trancher entre ces deux solutions. Elles imposent

[7] Notamment au travers de l'article 6.1.d du RGPD (sauvegarde des intérêts vitaux) ou encore l'article 9.2.i pour les données dites « sensibles », tous deux mis en parallèle avec le considérant 46 disposant que « Le traitement de données à caractère personnel devrait être également considéré comme licite lorsqu'il est nécessaire pour protéger un intérêt essentiel à la vie de la personne concernée ou à celle d'une autre personne physique. (…) Certains types de traitement peuvent être justifiés à la fois par des motifs importants d'intérêt public et par les intérêts vitaux de la personne concernée, par exemple lorsque le traitement est nécessaire à des fins humanitaires, y compris pour suivre des épidémies et leur propagation, ou dans les cas d'urgence humanitaire, notamment les situations de catastrophe naturelle et d'origine humaine. ».

[8] Le Règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 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, dit Règlement Général pour la Protection des Données (RGPD par la suite) exclut de son champ d'application les données anonymes. Voy. dans ce sens Consid. 26 in fine « Il n'y a dès lors pas lieu d'appliquer les principes relatifs à la protection des données aux informations anonymes, à savoir les informations ne concernant pas une personne physique identifiée ou identifiable, ni aux données à caractère personnel rendues anonymes de telle manière que la personne concernée ne soit pas ou plus identifiable. Le présent règlement ne s'applique, par conséquent, pas au traitement de telles informations anonymes, y compris à des fins statistiques ou de recherche. »

[9] Voy. *infra*.

[10] Voy. dans ce sens CEDP, Statement du 19 mars 2020.

[11] 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)

toutefois aux États membres de respecter le principe de proportionnalité appréciable par un contrôle juridictionnel opéré soit par la CJUE, soit par la CEDH[12].

Au sein du collectif TFC19, le potentiel liberticide d'un tel dispositif justifie, selon nous, un intérêt public impérieux *et* le consentement des personnes concernées.
Toutefois, dans l'hypothèse où le dispositif serait inefficace faute d'adhésion suffisante, le dispositif pourrait, *selon certains membres du collectif*, être généralisé sur le fondement de l'intérêt général. Cette position rejoint celle défendue par le professeur Zuboff, selon laquelle « les applications de contrôle de la pandémie doivent être obligatoires ». Elle opère une distinction claire entre les systèmes de surveillance d'oppression et les systèmes de surveillance appartenant à l'univers des systèmes sanitaires : « cela fait plusieurs dizaines d'années que, dans l'univers des systèmes sanitaires, le terme surveillance a une portée complètement différente de celle que nous lui attribuons quand il est question de multinationales privées opérant sur le Web. Notamment en cas d'épidémies, un système de surveillance n'est pas du tout quelque chose que nous devons combattre. Il s'agit de garder la maladie sous contrôle et d'éviter de nouvelles victimes. C'est grâce à ces systèmes de surveillance que le secteur de la santé sera efficace »[13].

b. Un consentement libre et éclairé

Dans l'hypothèse où le développement d'une application numérique de gestion sanitaire se fonde sur le consentement des personnes, il est impératif que celui-ci soit libre, éclairé, univoque, et spécifique (article 5.1.a. et 6.a. du RGPD)[14].
Dans le contexte de crise, le caractère « libre » de ce consentement pourrait être remis en cause: ce consentement l'est-il vraiment dans une période où la pression sociale, médiatique, mais aussi des réseaux sociaux, influe largement la population ?
Aussi, il est indispensable qu'il soit basé sur un geste actif émanant de la volonté propre de l'utilisateur. L'acceptation individuelle évite – ou à tout le moins réduit - le sentiment de suivi, d'intrusion dans la sphère intime, ou encore l'impression d'être tracé, pour l'individu qui le met en œuvre, étant entendu que cette application est un moyen de limiter la propagation du virus, pas de la réduire à néant.

[12] CEPD, Statement du 19 mars 2020, §1.3.
[13] S. ZUBOFF: «Les applications de contrôle de la pandémie doivent être obligatoires, comme les vaccins», *Le Figaro*, 17 février 2019 [en ligne] https://www.lefigaro.fr/international/shoshana-zuboff-les-applications-de-controle-de-la-pandemie-doivent-etre-obligatoires-comme-les-vaccins-20200417
[14] Voy. dans ce sens les lignes directrices 259 rév.01 (pas disponible en ligne)

Il est encore de prévenir tout « risque de discrimination, voire de stigmatisation » envers les personnes signalées par le dispositif et à l'encontre de celles qui n'ont pas acquiescé au traitement, conformément aux recommandations du Comité national pilote d'éthique du numérique[2]. Ce dernier souligne également le risque de déficit d'acceptabilité des mesures de suivi et l'adoption de comportements contestataires produisant l'effet inverse de l'objectif recherché[16].

c. Le droit d'opposition.

Le **droit d'opposition**, le premier des deux droits de la personne concernée découlant consentement, consacré par l'article 21 du RGPD se trouve transposé de multiples manières dans la présente hypothèse. Tout d'abord, le droit d'opposition se manifeste par le contrôle dont dispose la personne concernée, utilisatrice de l'application de trac(k)ing. Cette dernière doit pouvoir éteindre l'application de son propre choix ou encore la désinstaller à sa discrétion. De plus, ce dernier doit pouvoir effacer toutes les données qui se trouvent hébergées sur son téléphone, voire celles qui se trouvent sur le serveur centralisé.

Néanmoins, le **droit de portabilité**, l'autre droit de la personne concernée découlant consentement, consacré par l'article 20 du RGPD semble pas applicable dans la présente crise.

2. Finalité du traitement

Dans tout dispositif algorithmique, les finalités de la collecte et des traitements sont **orientées vers la gestion et sortie de crise** ; les données à caractère personnel collectées et traitées sont restreintes et limitées à cette stricte finalité[17]. La pertinence des traitements se fonde à cet effet sur les décisions des autorités publiques, et/ou les recommandations des autorités sanitaires compétentes.

---

[16] COMITÉ NATIONAL PILOTE D'ÉTHIQUE DU NUMÉRIQUE, « Réflexions et points d'alerte sur les enjeux d'éthique du numérique en situation de crise sanitaire aigüe », *Bulletin de veille n°1*, 7 avril 2020, pp. 10-11. https://www.ccne-ethique.fr/sites/default/files/publications/bulletin-1-ethique-du-numerique-covid19-2020-04-07.pdf

[17] Conformément au **principe de limitation des finalités** (les finalités sont déterminées à l'avance, explicites et légitimes article 5.1.b. du RGPD) et au **principe de minimisation des données à caractère personnel** (collecter restreinte aux données personnelles adéquates, pertinentes et limitées à ce qui est strictement nécessaire au regard des finalités préalablement déterminées article 5.1.c. du RGPD).

Tout dispositif algorithmique ne peut, de surcroît, et conformément à la recommandation de la Commission européenne, être utilisé à des fins répressives[18].
Tout dispositif algorithmique respecte toutes les préconisations récentes établies par le Comité européen de la protection des données (CEPD) relatif à la protection de la vie privée par défaut (« privacy by default »).

3. Fin du dispositif

Tout dispositif algorithmique est déployé à titre exceptionnel. Il détermine, en amont de son entrée en application, un **critère d'événement calendaire** de sortie de crise déterminant **la fin du dispositif**.
La fin du dispositif est expressément inscrite dans la loi.

> ⚖ L'observation de ce principe doit garantir une atteinte **justifiée et proportionnée** de la **restriction à l'exercice des libertés** et **droits fondamentaux**. La Commission européenne, se fondant sur la Charte des droits fondamentaux de l'Union européenne, l'a rappelé : ces restrictions, limitées au strict nécessaire, ne doivent pas perdurer la crise passée, sans raison valable[19].
>
> Cette exigence participe également au respect le principe de **limitation de la conservation des données** (article 5.1.e. du RGPD). Ce principe a été rappelé par le Contrôleur européen de la protection des données, lequel exige que les dispositifs technologiques mis en place pour lutter contre l'épidémie soient temporaires et ne perdurent pas après la crise[20].

---

[18] COMMISSION EUROPÉENNE, *Recommendation of 8.4.2020 on a common Union toolbox*, précédemment citée.

[19] C(2020) 2296 final, précédemment citée.
[20] W. WIEWIÓROWSKI, EU Digital Solidarity: a call for a pan-European approach against the pandemic, April 6th 2020.
https://edps.europa.eu/sites/edp/files/publication/2020-04-06_eu_digital_solidarity_covid19_en.pdf
Dans le même sens : EUROPEAN DATA PROTECTION BOARD, Statement on the processing of personal data in the context of the COVID-19 outbreak. Adopted on 19 March 2020.
https://www.dalloz-actualite.fr/sites/dalloz-actualite.fr/files/resources/2020/03/statement_2020_processing_personal_data_and_covid-19_en.pdf

🛠 Sur le plan technique, le collectif TFC19 recommande que le critère d'événement défini soit implémenté dans un ***smart contract*** et activé par un **oracle** de type « tiers de confiance », dont le nombre sera égal ou supérieur à trois.

Il préconise également la **procédure automatique d'anonymisation complète et irréversible** des données collectées. L'ensemble de la procédure pourrait, à cet effet, être tracé et auditable depuis une **blockchain publique**.

4. Géolocalisation partagée et/ ou anonymisée

Conformément aux recommandations du CEPD, **la collecte automatique de données de géolocalisation est interdite.**
L'autorité européenne insiste qu'une telle collecte ne respecterait pas le principe de minimisation des données[21].

⚖ Dans l'état actuel du droit, de nombreuses zones d'ombre entourent les pratiques de géolocalisation. Par principe prohibées du fait de leur caractère hautement intrusif dans la vie privée, les données personnelles de géolocalisation doivent respecter un formalisme important. Force est de souligner que dans le présent contexte, les données personnelles de géolocalisation doivent être interprétées comme étant l'utilisation pour une finalité tierce à celle de la fourniture des télécommunications par un opérateur téléphonique.

Pour la localisation des citoyens dans le cadre de la présente, le Comité européen insiste sur une obligation des États membres à rechercher les modalités d'anonymiser à travers une agrégation des données. Cette agrégation remplirait ainsi deux objectifs : celui de cartographier le nombre d'appareils mobiles dans une zone géographique définie tout en excluant lesdites données de l'empire du RGPD[22]. Dans

[21] CEPD, lettre du 14 avril 2020, « Collecting an individual's movements in the context of contact tracing apps would violate the principle of data minimisation. In addition, doing so would create major security and privacy risks ».
[22] COMITÉ EUROPÉEN POUR LA PROTECTION DES DONNÉES, « Statement on the processing of personal data in the context of the COVID-19 outbreak », 19 mars 2020, disponible sur https://edpb.europa.eu/our-work-tools/our-documents/other/statement-processing-personal-data-context-covid-19-outbreak_en , spéc. p.2« *Public authorities should first seek to process location data in an anonymous way (ie. processing data aggregated in a way that individuals cannot bere-identified), which could enable generatingreports on the*

une telle configuration, les données de géolocalisation ne permettraient pas une réidentification de la personne concernée lui offrant ainsi des garanties sur le respect des droits.

Dans l'hypothèse où les données ne sont pas anonymisées, le principe de minimisation des données évoqué précédemment (article 5.1.c. du RGPD) exige que seules les données nécessaires pour atteindre les finalités déterminées soient collectées et traitées. Ce **principe de nécessité** requiert le recours aux techniques les moins attentatoires aux droits et libertés fondamentaux pour atteindre l'objectif poursuivi[23]. Il doit être noté que le CEPD insiste sur les « circonstances exceptionnelles » pour accorder une marge d'appréciation plus importante aux États membres. En effet, l'autorité européenne des données estime que l'appréciation des modalités du principe de nécessité se fera en fonction des modalités du traitement. Cette marge de manœuvre est tempérée par le caractère strictement temporaire du traitement envisagé entraînant des limitations de la gestion des données à caractère personnel dans son exécution[24].

Le caractère nécessaire de la collecte automatique des données de géolocalisation est débattu dans ce cadre. Si le CEPD affirme que les mesures invasives – telles que le traitement de données de localisation non-anonymisées – pourraient être considérées comme proportionnées dans des circonstances exceptionnelles et en fonction des modalités concrètes du traitement, il précise que ces mesures devront nécessairement prévoir des garanties renforcées (proportionnalité de la mesure en termes de durée et de portée, limitation de la conservation des données et de la finalité)[25].

Par principe, et en dehors de procédures pénales, la mise en œuvre du traitement **de données de localisation non-anonymisées** par les opérateurs télécoms – ou des applications mobiles – est soumise au consentement des personnes concernées (article

concentration of mobile devices at a certain location ("cartography"). Personal data protection rules do not apply to data which has been appropriately anonymised »

[23] COMITÉ EUROPÉEN POUR LA PROTECTION DES DONNÉES, « Statement on the processing of personal data in the context of the COVID-19 outbreak », 19 mars 2020, disponible sur https://edpb.europa.eu/our-work-tools/our-documents/other/statement-processing-personal-data-context-covid-19-outbreak_en

[24] « *however, it should be subject to enhanced scrutiny and safeguards to ensure the respect of data protection principles (proportionality of the measure in terms of duration and scope, limited data retention and purpose limitation)* ». *Ibidem* p. 3,

[25] *Ibidem.*

9 de la Directive ePrivacy). Toutefois, comme nous l'avons déjà évoqué, le consentement pourrait s'avérait, au regard des circonstances, insuffisamment protecteur[26].

À défaut de consentement, et en l'absence d'anonymisation, le CEPD insiste sur le fait que la collecte et le traitement des données de localisation par les opérateurs télécoms - ou des applications mobiles - peuvent être **autorisés par la loi sur le fondement de la sécurité publique** (article 15 de la Directive ePrivacy)[28]. Cette disposition fait aujourd'hui défaut dans le contexte de crise sanitaire actuelle, les garanties démocratiques apparaissant ainsi insuffisantes. En effet, et sur la base de la jurisprudence de la Cour européenne des droits de l'homme[29], l'autorité européenne insiste sur ce dernier point en conditionnant le recours à la loi pour passer outre le consentement par un droit à un recours juridictionnel des citoyens.

La transmission par les opérateurs téléphoniques des données de localisation aux autorités pour des motifs sanitaires n'est pas prévue par les dispositions nationales. Seul l'article L 851-1 du Code de la Sécurité intérieure (CSI) prévoit la transmission par les opérateurs téléphoniques des données de localisation aux services de renseignement, celle-ci doit être justifiée « par les menaces, les risques et les enjeux liés aux intérêts fondamentaux de la nation mentionnées à l'article L. 811-3 » (article L.801-1 4°). Or, la protection de la santé publique pourrait être comprise à ce titre, mais ni la loi renseignement de 2015, ni l'étude d'impact du 18 mars 2015, n'y font mention.

Une intervention du législateur reste donc indispensable pour mettre en œuvre tout dispositif de *tracking* – en l'absence de consentement et d'anonymisation irréversible – justifié par des motifs sanitaires.

🛠 Sur le plan technique, le collectif TFC19 recommande que toutes les technologies relatives à la **collecte automatique** de données de géolocalisation permettant le

[26] Telle est notamment l'inquiétude formulée par le Comité national pilote d'éthique du numérique français, qui redoutent que le consentement au traitement des données de géolocalisation ne soit ni libre ni éclairé en raison de la pression sociale, de l'imitation des proches ou du *nudging*. COMITÉ NATIONAL PILOTE D'ETHIQUE DU NUMÉRIQUE, « Réflexions et points d'alerte sur les enjeux d'éthique du numérique en situation de crise sanitaire aigüe », *Bulletin de veille* n°1, 7 avril 2020, p. 11.

[28] COMITÉ EUROPÉEN POUR LA PROTECTION DES DONNÉES, « Statement on the processing of personal data in the context of the COVID-19 outbreak », note supra, p. 2.

[29] Cour Européenne des Droits de l'homme, *Klass c. Allemagne*, 06 sept. 1972.

tracking à partir des smartphones (*notamment pour réaliser le contact tracing*) soient **exclues du dispositif adopté**.

Il peut toutefois être admis, **si l'utilisateur le souhaite**, de transmettre sa géolocalisation depuis son terminal selon la **méthode dite *"location update callback"***. L'avantage d'une telle méthode est de notifier tout changement significatif de localisation (unité de distance variable définie par l'utilisateur) sans diffuser en temps réel sa géolocalisation. Un dispositif permettant à l'utilisateur d'autoriser - ou non - le partage de chaque information peut répondre à ses exigences.

Il peut également être envisagé, à ces mêmes fins, que l'utilisation du **Bluetooth** soit activée **uniquement à la demande de l'utilisateur** et pour une détection **ponctuelle** des autres terminaux environnants. Les interfaces de communication Bluetooth exposent en effet potentiellement l'utilisateur à un risque élevé de piratage, car elles rendent le terminal vulnérable aux sollicitations extérieures non consenties.

En conclusion, le collectif TFC19 préconise une application "*user centric*", qui implique :

- ✓ L'absence de consentement général pour l'ensemble des usages du dispositif ;
- ✓ La maîtrise de l'information transmise par l'utilisateur (déclaratif) ;
- ✓ La possibilité d'une anonymisation de la donnée de géolocalisation à l'initiative de l'utilisateur par la dégradation de ses coordonnées (ex: élargissement du périmètre).
- ✓ La possibilité de mettre en œuvre un système Bluetooth à la demande de l'utilisateur ; respectueux de ses droits et protégeant sa vie privée.

5. Profilage

Un **profilage** des individus de **type « social »**, étranger aux finalités du traitement, élaboré à partir des données à caractère personnel qui auraient été collectées, est **interdit**.

Le profilage consiste en l'extrapolation des données disponibles sur le dispositif au moyen de processus de collecte automatisée d'informations, visant à reconstruire des profils et les appliquer pour des traitements secondaires[30].

Sont prohibés les profilages sociaux visant, par exemple, à distinguer les citoyens « vertueux », « intègres » ou tout autre profil fondé sur des valeurs morales, à partir des jeux de données collectées ou en croisant ceux-ci avec d'autres jeux.

⚖ La pratique du profilage ne fait pas l'objet d'une interdiction expresse. Le RGPD indique seulement que la personne concernée par le traitement a le droit « de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire » (article 22).
Les dangers de cette pratique ont toutefois, de longue date, été identifiés par la doctrine[31], et le Conseil des droits de l'homme des Nations Unies a relevé que « le traitement automatique des données à caractère personnel pour l'établissement de profils individuels peut aboutir à une discrimination ou à des décisions pouvant avoir des conséquences sur la réalisation des droits de l'homme, notamment les droits économiques, sociaux et culturels »[32]. La principale difficulté procède de la décontextualisation des données. Leur réutilisation à de nouvelles fins peut nuire à l'autonomie d'information de la personne concernée. Le Conseil de l'Europe relève en ce sens que le profilage « a une incidence directe sur le droit d'une personne à l'autodétermination de son information »[33].

La réutilisation des données dans le cadre d'un profilage peut également être incomplète, inexacte ou dépassée et présenter ainsi une fausse image des individus

[30] Voy. dans ce sens la définition fournie par le considérant 71 du RGPD.
[31] M. HILDEBRANDT and S. GUTWIRTH. "General Introduction and Overview", in *Profiling the European Citizen*. Springer, Dordrecht, 2008, pp. 1–13.
https://link.springer.com/chapter/10.1007/978-1-4020-6914-7_1
[32] Résolution du Conseil des droits de l'homme des Nations Unies sur le droit à la vie privée à l'ère du numérique, Doc. A/HRC/34/7, 23 Mars 2017, §.17. https://www.right-docs.org/doc/a-hrc-res-34-7/
Voy. également la recommandation du Conseil de l'Europe qui analyse les risques afférents : *La protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage*, Recommandation CM/Rec(2010)13 adoptée par le Comité des Ministres du Conseil de l'Europe le 23 novembre 2010, https://rm.coe.int/16807096c4
[33] *Algorithmes et droits humains*, Etude du Conseil de l'Europe, DGI (2017) 12, p.17.
https://rm.coe.int/algorithms-and-human-rights-fr/1680795681

pouvant leur être préjudiciable[34]. Se référant aux dernières déclarations de l'Organisation mondiale de la santé[35], la Commission européenne avertit en ce sens le risque stigmatisation des personnes identifiées comme malades sur le fondement de données inexactes[36].

Plus globalement, seuls les cas prévus par le RGPD, notamment à des fins de recherche scientifique ou d'exercice de droits en justice[37], et mettant en œuvre des garanties suffisantes, peuvent faire l'objet d'une réutilisation des données à caractère personnel.

🛠 Sur le plan technique, le groupe TFC19 recommande que :

- ✓ La structure des données transmises aux autorités compétentes n'autorise pas l'agrégation des données permettant un profilage de type social.
- ✓ La structure des données ne permette pas davantage une réutilisation des données en dehors des cas expressément prévus par le RGPD (recherche scientifique et/ou exercice des droits en justice)
- ✓ Les solutions techniques développées au service de la traçabilité et de l'auditabilité permettent de contrôler l'observation, par les utilisateurs autorisés, de ces interdictions.

6. Transparence, traçabilité, auditabilité

Tout dispositif algorithmique est **transparent**, **traçable et auditable**.
Les audits algorithmiques reposent conjointement sur :

- Des **garanties techniques** assurant la transparence du code, et la traçabilité des données comme des usages ;
- Des **garanties humaines** pour l'usage de chaque outil du dispositif, assurées par des collèges d'évaluation *ad hoc*.

Ces garanties :

[34] *Ibidem.*
[35] ORGANISATION MONDIALE DE LA SANTÉ, « Outil de l'OMS pour l'analyse des comportements face à la COVID-19 », dernière consultation le 10 avril 2020, http://www.euro.who.int/fr/health-topics/health-emergencies/coronavirus-covid-19/novel-coronavirus-2019-ncov-technical-guidance/who-tool-for-behavioural-insights-on-covid-19
[36] C(2020) 2296 final, précédemment citée.
[37] Voy. ici le considérant 50 du RGPD.

- Assurent la **conformité** des dispositifs à l'état de droit en général, au respect des finalités identifiées et désignées en particulier ;
- Préviennent et corrigent l'existence ou l'apparition de **biais algorithmiques** ;
- Seules les **personnes autorisées** peuvent accéder aux données[38].

⚖ *Traçabilité et conformité*

La traçabilité est un gage de transparence : elle permet de prévenir et identifier tout usage dévoyé des données par rapport aux finalités initialement prévues. Les données doivent être traitées de manière à garantir une sécurité et une confidentialité appropriées, y compris pour prévenir l'accès non autorisé à ces données, à l'équipement utilisé pour leur traitement ainsi qu'à l'utilisation non autorisée de ces données et de cet équipement (considérant (39) du RGPD).

La traçabilité des usages et des données constitue par suite, et plus largement, une garantie quant à la conformité légale effective des dispositifs de traitement.

⚖ *Transparence*

Pour la Commission européenne, la transparence est essentielle en vue de gagner et conserver la confiance des utilisateurs d'un dispositif algorithmique volontaire[45]. Au regard du climat de suspicion entourant l'usage des technologies dites « de surveillance », les garanties de transparence apparaissent décisives sur le terrain de l'acceptabilité sociale du dispositif et par suite, de son succès.
Dans le même sens, le CEPD invite les États à fournir un effort de pédagogie et de transparence[46]. Un dispositif d'information, parfois même de vulgarisation, est selon lui, la clef de voûte d'une mise en œuvre respectueuse des droits et libertés des individus[47].

---

[38] Le Conseil de l'Europe préconise en ce sens, dans le cadre des traitements de données de santé, la mise en place de « mesures destinées à contrôler les accès aux bases de données et aux données elles-mêmes, en s'assurant que seules les personnes autorisées peuvent y accéder ». Recommandation CM/Rec (2019)2, point 13.4

[45] Voy. également dans ce sens le CEPD letter du 14 avril 2020, §1.3.

[46] Voy. *infra.*

[47] Voy. dans ce sens, CEPD, lettre du 14 avril 2020, *« These laws could be accompanied by appropriate communications activities at national level to promote such tools, with awareness-raising campaigns and assistance to minors, to the impaired, or to less skilled or educated parts of the population, in order to avoid scattered adoption,*

Au sein du collectif TFC19, nous jugeons, à ce titre, indispensable de rendre **obligatoire la publication de l'analyse d'impact** réalisée (PIA - *Privacy Impact Assessment*). Un résumé de celle-ci, accessible au grand public, devrait accompagner sa communication.

⚖ *Auditabilité et contrôle*

L'auditabilité des dispositifs algorithmiques n'est pas expressément prévue par le RGPD. Toutefois, elle constitue un moyen d'assurer le principe de loyauté et de transparence (article 5.1.a. du RGPD). Elle pourrait s'analyser par extension comme une mesure technique appropriée afin de garantir un niveau de sécurité adapté au risque (article 32 du RGPD). L'auditabilité procède également d'une lecture conjointe des articles 22, 13 et 15 du RGPD – relatifs au droit d'accès aux données collectées et au droit de connaître la finalité de traitement – qui confère, selon certains auteurs un « droit d'explication »[48].
Dans cette perspective, le CEPD recommande la mise à disposition, en **libre accès** des dispositifs, offrant à tout tiers intéressé les modalités de contrôle[49].

Au sein du collectif TFC19, il nous apparaît plus largement fondamental de consacrer « **un droit d'audit** » des dispositifs. Ce droit devra évidemment être accordé à la CNIL, conformément à la loi, mais également à des organisations dont la mission est de protéger les droits des citoyens. Nous pensons aux ONG telles que la Ligue des droits de l'homme ou Amnesty International, ainsi qu'aux associations de consommateurs nationales agréées.
Dans l'exercice de ce droit d'audit, lesdites associations devraient pouvoir se faire assister par des « prestataires d'audit de la sécurité des systèmes d'information » (PASSI) qualifiées par l'Agence nationale de la sécurité des systèmes d'information (ANSSI), et ce aux frais de l'État. »

---

or blurred knowledge of the evolution of the epidemics and any potential health divide. Indeed, anylack of data, due to individuals' inattentive use of the app or even to battery fault of the device may seriously undermine the overall public usefulness of these instruments. »

[48] B. GOODMAN et S. FLAXMAN, "European Union regulations on algorithmic decision- making and a "right to explanation"", *AI Magazine*, fall 2017, p. 50-57.

[49] Voy. dans ce sens les préconisations du ehealth toolbox, spéc. p.31 ; également la lettre du 14 avril 2020 du CEPD « *the source code should be made publicly available for the widest possible scrutiny by the scientific community.* ».

🛠 Au sein du collectif TFC19, nous insistons sur l'importance de l'architecture permettant à tout « tiers de confiance » de contrôler a posteriori le respect effectif par l'Etat (les autorités sanitaires), responsable de traitement, des garanties promises (notamment l'anonymisation définitive à la sortie de crise). À cet effet, nous formulons, les recommandations techniques suivantes:

Premièrement, tous les algorithmes de traitement appliqués aux données collectées par tout dispositif seront en **libre accès** et devront :

- ✓ Répondre aux critères de conformité définis ;
- ✓ Permettre les audits par les **tiers de confiance.**

Deuxièmement, tout dispositif algorithmique doit intégrer nativement une **procédure de traçabilité.**

Celui-ci pourrait être établi entre les différents registres serveurs dudit dispositif et une **blockchain publique**. Un tel dispositif permettrait de générer le condensat par bloc d'événements relatifs aux fichiers logs du système d'exploitation serveur, ainsi que ceux des bases de données interfacées. Ces hashs seraient enregistrés dans une blockchain publique et auditable par comparaison entre les hashs rétrocalculés en local à partir des fichiers logs et des hashs présents dans la blockchain publique.

Troisièmement, nous recommandons que les données collectées - comme leur leurs usages – soient traçables par tout dispositif qui générera le condensat des données collectées (anonymisées ou à caractère personnel) par bloc. Les usages pourraient en effet être tracés et auditables par les fichiers logs corrélés aux hashs de la blockchain publique.

⚖ *Le nécessaire contrôle humain*.

L'article 22 du RGPD précité (*cf.* 5. Profilage) prévoit un droit général à l'intervention humaine dans le cadre de prise de décision fondée sur un traitement automatisé de données à caractère personnel et produisant des effets juridiques à l'égard d'une

personne ou l'affectant de manière significative. Pour autant, les garanties humaines sont, à ce jour, envisagées pour certains traitements seulement[50].

Au sein du collectif TFC19, nous soutenons qu'une attention particulière doit être accordée aux garanties humaines en complément des garanties techniques.
Le projet de loi française relatif à la bioéthique, qui envisage de rendre les garanties humaines obligatoires en matière de santé, constitue de ce point de vue une belle piste de réflexion. Son article 11 prévoit de compléter, à la suite des travaux expérimentaux de David Gruson en la matière[51], l'article L. 4001-3 du code de la santé publique par les dispositions suivantes :

> « Art. L. 4001-3. – I. – Lorsque, pour des actes à visée préventive, diagnostique ou thérapeutique, est utilisé un traitement algorithmique de données massives, le professionnel de santé qui communique les résultats de ces actes informe la personne de cette utilisation et des modalités d'action de ce traitement.
> « II. – L'adaptation des paramètres d'un traitement mentionné au I pour des actions à visée préventive, diagnostique ou thérapeutique concernant une personne ne peut être réalisée sans l'intervention d'un professionnel de santé.
> « III. – La traçabilité des actions d'un traitement mentionné au I et des données ayant été utilisées par celui-ci est assurée et les informations qui en résultent sont accessibles aux professionnels de santé concernés. »

Sur le modèle de ce projet, nous recommandons que les dispositifs de traitement des données à caractère personnel intègrent des garanties humaines. Celles-ci se traduiraient par **l'évaluation régulière des différents outils** des dispositifs en question par des collèges *ad hoc*, composés de professionnels de santé, d'experts et de représentants de la société civile reflétant un pluralisme des intérêts.

---

[50] A titre d'exemple, il en est ainsi en France des services en ligne de conciliation ou de médiation qui ne peuvent avoir pour seul fondement un traitement algorithmique ou automatisé de données à caractère personnel (article 4-5 de la loi du 18 novembre 2016 de modernisation de la justice du XXIe siècle).
Notons également quen, selon le Conseil constitutionnel français, seules les décisions individuelles dont « les principes de fonctionnement d'un algorithme ne peuvent être communiqués sans porter atteinte à l'un des secrets ou intérêts énoncés au 2° de l'article L. 311-5 du code des relations entre le public et l'administration » ne peuvent être prise sur le fondement exclusif de cet algorithme . En d'autres termes, toute autre forme de décision administrative peut être adoptée sans intervention, et, par extension, sans garantie d'une intervention humaine. Cons. const., 12 juin 2018, n° 2018-765 DC, D. 2019. 1248, obs. E. DEBAETS et N. JACQUINOT ; AJDA 2018. 1191 ; RTD eur. 2018. 830, obs. D. RITLENG.

[51] « Algorithme en santé: le médecin devrait informer son patient lorsqu'il a recours à une IA», *Le Figaro*, 4 janvier 2019, https://www.lefigaro.fr/sciences/2019/01/04/01008-20190104ARTFIG00257-algorithme-en-sante-le-medecin-devrait-informer-son-patient-lorsqu-il-a-recours-a-une-ia.php

7. Anonymisation

Tout dispositif algorithmique offre et garantit une stricte **anonymisation** des données à caractère personnel :

- Totale ou partielle pendant la crise ;
- Irréversible après la crise.

⚖ Pendant la crise, et conformément aux recommandations de la Commission européenne[52], il est essentiel :

- ✓ De privilégier les **mesures efficaces les moins intrusives**, telles que l'utilisation de données anonymisées,
- ✓ Ou, à tout le moins, de proposer des **garanties appropriées** telles que la pseudonymisation, l'agrégation, le chiffrement et la décentralisation.

Après la crise, il s'agira de respecter le principe de **limitation de la conservation des données** imposé par le RGPD en vertu duquel « les données à caractère personnel doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées » (article 5.1.e.).
Le Conseil de l'Europe recommande dans le même sens que « l'anonymisation [soit] pratiquée dès lors que les objectifs poursuivis par les recherches scientifiques le permettent »[53].

🛠 Sur le plan technique, il nous semble indispensable que les garanties en matière d'anonymisation des données ***en local*** (avant envoi) permettent un transfert des données anonymisées vers les serveurs de collecte.
L'anonymisation des données en phase de collecte initiale pourrait être garantie selon les règles suivantes :
(i) tous les champs relatifs à l'identité civile d'un utilisateur sont inexistants ;
(ii) un identifiant anonyme est attribué à chaque utilisateur ;

[52] *Ibidem.*
[53] Recommandation CM/Rec(2019)2, point 15.9. https://www.apda.ad/sites/default/files/2019-03/CM_Rec%282019%292F_FR.pdf

(iii) toute donnée (ou métadonnée) permettant l'identification indirecte d'un utilisateur est systématiquement anonymisée[54].

Il apparaît également nécessaire, comme déjà mentionné, que le **code source des interfaces de collecte** de données soit **en libre accès** et donc auditable par un tiers. Les transmissions pourraient être automatiquement tracées et auditables à partir d'une blockchain publique. Enfin, les autorités compétentes pourraient ainsi, au besoin, solliciter l'identité rattachée à ces données via le terminal de communication de l'utilisateur.

8. Souveraineté numérique

Les données sont centralisées sur des serveurs nationaux ou européens garantissant l'exercice de la **souveraineté numérique** de l'État.

⚖️ Cette garantie permet notamment d'échapper à l'extraterritorialité de certains droits à l'instar du droit américain, en vertu duquel les prestataires de services établis aux États-Unis doivent fournir les données stockées sur leurs serveurs. La transmission intervient en cas d'injonction des autorités américaines, « indépendamment du fait que les enregistrements, les communications et les autres informations se situent en dehors du territoire des États-Unis » (Cloud Act §103(a) et 18 U.S.C §2713).

🛠️ Sur le plan technique, tous les serveurs relatifs au dispositif mis en œuvre devront être hébergés par un opérateur national ou européen et localisés sur ce même territoire.
L'agrément ou certificat HDS (hébergement des données de santé) prévu par l'article L.1111-8 du code de la santé publique français, offre à cet égard des pistes de réflexion intéressantes[55].

[54] Voy. Synthèse technique *infra*.
[55] Voy. en ce sens : Explicitation du champ d'application du cadre juridique de l'hébergement de données de santé par le ministère chargé de la Santé, représenté par la Délégation à la stratégie des systèmes d'information de santé, 16 mai 2019 [en ligne]
https://esante.gouv fr/sites/default/files/media_entity/documents/FAQ%20HDS_16052019_V0%2018.pdf

9. Conservation et vente des données

La **vente à des tiers** des données à caractère personnel collectées par tout dispositif est interdite.

⚖ Les enjeux de santé publique excluent tout usage commercial des données à caractère personnel. Le Contrôleur européen de la protection des données a exigé, à ce titre, que l'accès aux données soit limité[56]. La Commission européenne a également rappelé, l'impérieuse nécessité de cette limite en invitant les Etats à veiller à ce que les données ne soient pas utilisées à des fins commerciales[57].

Rappelons par ailleurs que selon le Conseil de l'Europe « les compagnies d'assurances ne peuvent pas être considérées comme des destinataires autorisés à accéder aux données relatives à la santé des personnes » en l'absence de dispositions légales assorties de garanties[58].

🛠 Sur le plan technique, des garanties élevées en matière de transparence et d'auditabilité doivent être exigées. Le collectif TFC19 préconise notamment, à cet effet, d'interfacer les procédures de traçabilité à tous les serveurs du dispositif, ainsi qu'aux applications de traitement de la donnée collectée.
L'horodatage et l'intégrité des hashs étant infalsifiables, la blockchain publique est susceptible de limiter les usages prohibés et garantira par la même un contrôle efficace de ceux-ci.

10. Alternative(s) au numérique

Tout dispositif algorithmique garantit **l'égalité devant le service public** ; des **solutions alternatives au numérique** sont proposées.

⚖ Conformément aux exigences constitutionnelles, tout dispositif doit garantir l'égalité devant le service public et de ne pas créer de discriminations - selon les

[56] W. WIEWIÓROWSKI, "EU Digital Solidarity: a call for a pan-European approach against the pandemic", précédemment cité.
[57] C(2020) 2296 final, précédemment citée, n°10(1).
[58] Recommandation CM/Rec(2019)2, point 9.2

terminaux utilisés - dans la jouissance des droits garantis par la Convention Européenne des Droits de l'Homme (article 14 de la CEDH).

Le défenseur des droits recommande à cet effet :

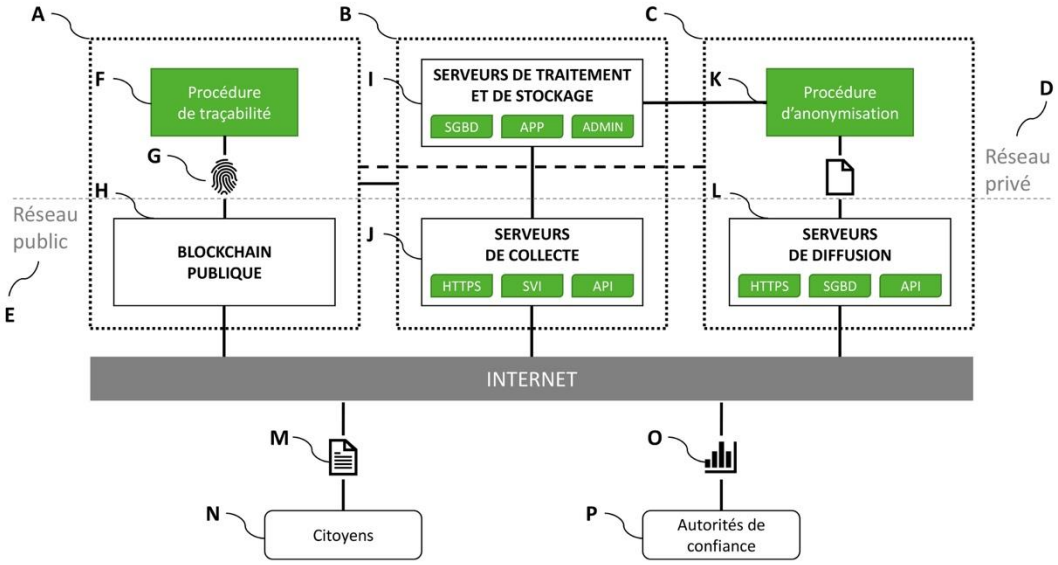
- La conservation de modalités d'accès aux services publics plurielles et alternatives à la voie dématérialisée ;
- La prise en compte, dans tout dispositif ou toute démarche, des difficultés potentiellement rencontrées par les usagers ;
- L'identification et l'accompagnement des personnes en difficulté avec le numérique ;
- La prise en compte des publics spécifiques (dans les établissements pénitentiaires, pour les majeurs protégés et les personnes handicapées)[59].

🛠 Le dispositif adopté devra être aussi accessible au plus grand nombre et proposer une passerelle alternative au smart phone, tel qu'un serveur vocal interactif ou une collecte indirecte des données auprès des autorités.

[59] *Dématérialisation et inégalités d'accès aux services public*, Rapport du Défenseur des droits, 2019. [en ligne] www.defenseurdesdroits.fr/sites/default/files/atoms/files/rapport-demat-num-21.12.18.pdf

III. SYNTHÈSE TECHNO-NORMATIVE

Figure 1. Proposition d'architecture technique



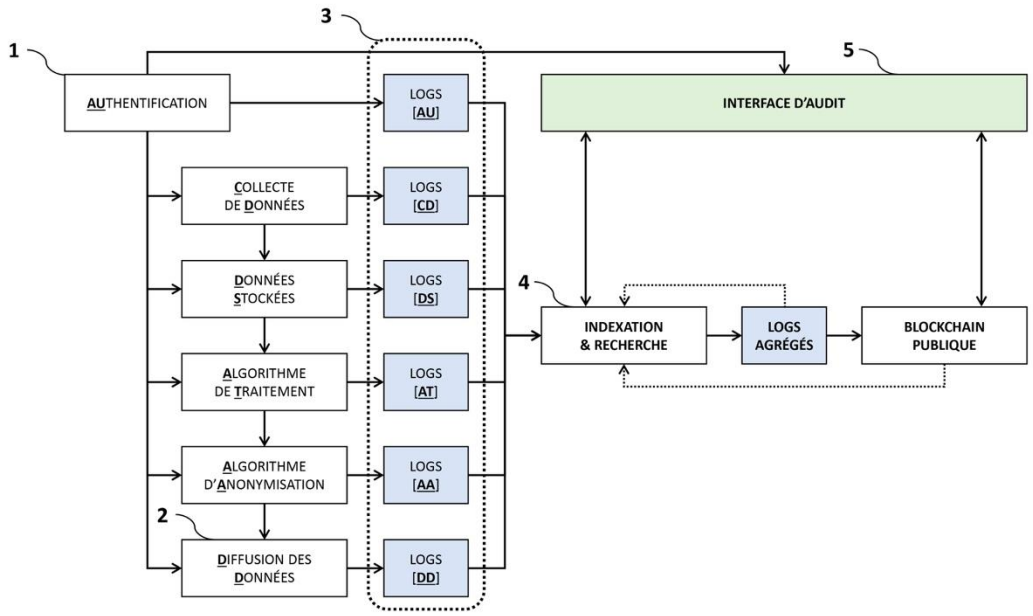
Source : TFC19

(A) Sous-dispositif technologique permettant de tracer et d'auditer à partir d'une blockchain publique : (i) la collecte de données ; (ii) les traitements opérés sur les données collectées ; (iii) les usages (partages et diffusion) des données traitées.

(B) Infrastructure de serveurs physiques et virtuels relative à la collecte et aux traitements des données. Cette infrastructure bénéficie d'un cloisonnement réseau entre **(D)** et **(E)** de type DMZ.

(C) Sous-dispositif technologique assurant l'anonymisation (totale ou partielle) des données **(K)** en vue d'une diffusion **(L)** auprès des utilisateurs autorisés **(P)** à exploiter les données **(O)**.

Figure 2. Procédure de traçabilité



Source : TFC19

Dans le cadre de la procédure de traçabilité proposée, le collectif TFC19 recommande une approche de développement dite **LDD (*log-driven development*)** afin d'orienter la programmation des modules dans l'unique objectif de générer des logs utiles (journal d'événements) et de garantir la traçabilité des usages desdits modules.

1 : AUTHENTIFICATION – Tout dispositif doit une authentification pour accéder aux différents services proposés par l'application proposée.

A ce jour, nous retenons quatre types d'accès :

(i) ***accès utilisateur*** (citoyen) ;

(ii) ***accès administrateur*** (personnel technique) ;

(iii) ***accès expert*** (autorités désignées par le gouvernement) ;

(iv) ***accès tiers de confiance*** (audit).

Les accès de type (ii), (iii) et (iv) nécessiteraient une authentification certifiée (exemple avec le ***certificat x509*** et HMAC) et les accès de type (i) se ferait à partir d'une méthode d'authentification sécurisée (exemple avec JWT et HMAC).

2 : DIFFUSION DES DONNÉES – Nous recommandons que les données partagées soient ***filtrées et segmentées en fonction du rôle et des besoins*** des autorités ayant accès au dispositif. Dans l'hypothèse où un utilisateur souhaiterait partager son identité réelle avec

certaines autorités, toute donnée relative à son identité réelle serait systématiquement chiffrée à partir de la ***clé publique des certificats x509 rattachés aux autorités concernées***. Ainsi, les données se rapportant à l'identité réelle d'un utilisateur seraient ***chiffrées de bout en bout*** et ne seront jamais connues du dispositif.

3 **: LOGS DU DISPOSITIF** – Le niveau de traçabilité recommandé par le collectif TFC19 serait rendu possible (notamment) par la ***collecte continue d'événements*** exécutés par l'ensemble des modules du dispositif. Ainsi, il deviendrait possible de retracer avec précision l'interaction entre une personne physique ou morale (citoyen, expert, administrateur et tiers de confiance) et un ou plusieurs modules du dispositif. Les interactions entre les différents modules internes au dispositif seraient également traçables. D'un point de vue technique, l'intégrité des logs du dispositif pourrait ainsi être garantie *a posteriori* par une blockchain publique.

4 : INDEXATION & RECHERCHE (logs) – Le module que nous recommandons a pour objectif de centraliser tous les logs générés par les différents modules du dispositif de manière structurée et intelligible (exemple avec la *stack Elasticsearch*). A partir des logs centralisés, un sous-module générerait un ***bloc de logs agrégés de taille fixe*** et calculerait le condensat (exemple avec SHA-256) dudit bloc pour l'inscrire sur une blockchain publique (exemple avec Ethereum et/ou Tezos).

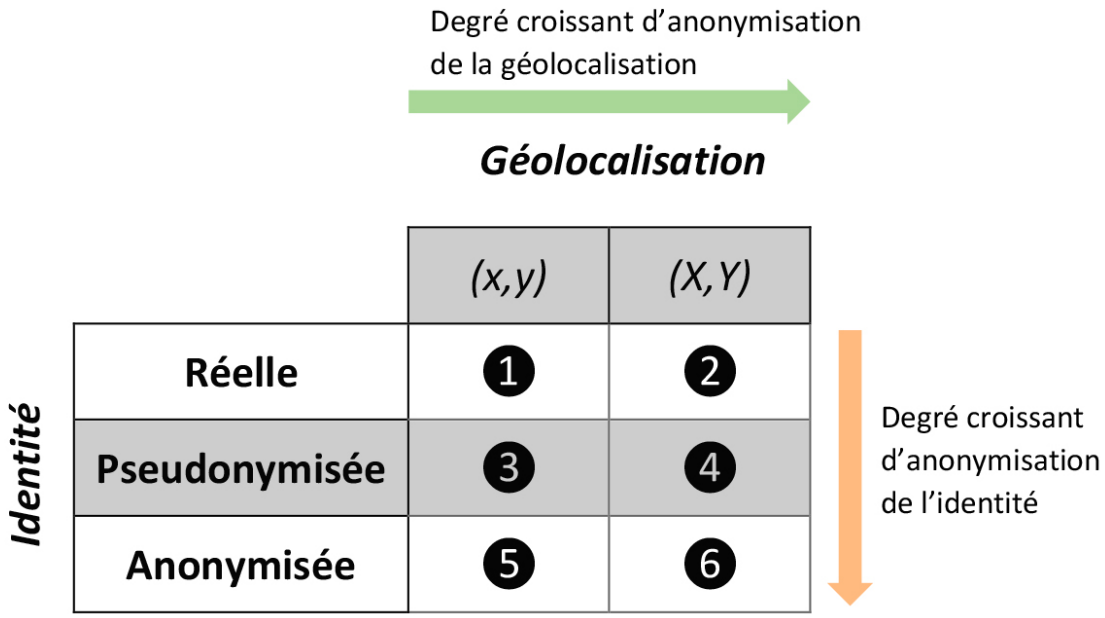
5 **: INTERFACE D'AUDIT** – L'interface que nous recommandons communiquerait directement avec le module d'indexation (logs centralisés) et la blockchain publique afin de rétro-calculer le condensat de certains blocs de logs avec le condensat correspondant inscrit dans le registre de la blockchain publique. L'auditeur autorisé pourrait ainsi ***contrôler tous les événements survenus*** au sein du dispositif et ***vérifier notamment l'intégrité des logs du dispositif*** comparativement aux valeurs enregistrées dans la blockchain publique.

Tableau 1. Table de correspondance entre garanties démocratiques et recommandations technologiques

	Briques technologiques du dispositif TFC19															
Garanties démocratiques	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
(1) Consentement	✓					✓	✓	✓		✓			✓	✓	✓	✓
(2) Finalité	✓					✓	✓	✓	✓		✓					
(3) Fin du dispostif								✓	✓		✓					
(4) Géolocalisation													✓	✓		
(5) Profilage	✓		✓						✓							
(6) Transparence	✓								✓							
(7) Anonymisation	✓										✓				✓	✓
(8) Souveraineté Numérique		✓		✓	✓	✓			✓	✓	✓				✓	✓
(9) Conservation et vente des données	✓	✓	✓			✓	✓	✓	✓	✓	✓	✓			✓	✓
(10) Alternative au numérique										✓				✓		

Source : TFC19

Tableau 2. Degré d'anonymisation : analyse croisée entre identité et géolocalisation



Source : TFC19

A noter que la présente matrice s'applique également pour l'interface Bluetooth.

Le présent schéma décrit les différentes hypothèses dans lesquelles peuvent s'inscrire le processus de pseudonymisation/anonymisation. Elles reposent sur deux variables : l'identité et la géolocalisation selon la granularité souhaitée de transmission.

① **L'identité réelle** d'un utilisateur ainsi que les **coordonnées de géolocalisation précises** sont connues du dispositif, idéalement après un ***consentement pas-à-pas*** de l'utilisateur (recommandation TFC19). Dans le cadre de tout dispositif – et dans l'hypothèse où celui-ci repose sur le consentement - l'utilisateur pourra décider de déclarer toute information utile auprès des autorités sanitaires dans le but de bénéficier d'une assistance *ad hoc*. ② L'Identité réelle d'un utilisateur est connue du dispositif et la donnée de géolocalisation est dégradée. ③ L'identité est pseudonymisée et la donnée de géolocalisation est précise. ④ L'identité est pseudonymisée et la donnée de géolocalisation est dégradée. ⑤ L'identité d'un utilisateur est anonymisée – ***réidentification par individualisation, corrélation et inférence à partir des données collectées/traitées est impossible*** – et la donnée de géolocalisation est précise (dans le respect du processus d'anonymisation). ⑥ L'identité d'un utilisateur est anonymisée et la donnée de géolocalisation est dégradée.