Point d'étape sur les activités de la CNIL dans le contexte de la COVID-19

Le rôle du régulateur et les enjeux de la crise sanitaire en termes de protection des données

Rapport présenté en séance plénière
le 12 novembre 2020

Rapporteure : Mme Valérie PEUGEOT

Avec le concours de :

Mme Nacera BEKHAT, Juriste au service des affaires économiques

MM. Antoine COURMONT et Régis CHATELLIER, Chargés d'études prospectives au PIEP

ainsi que le **Groupe de travail interne « COVID -19 »**

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Table des matières

Introduction

La crise sanitaire a notamment eu pour effet de placer les enjeux de protection des libertés fondamentales et des données personnelles au cœur des débats publics. Elle a également fait émerger de nombreux points de tensions susceptibles de déplacer les perceptions et préoccupations concernant la protection des données personnelles et plus généralement de la vie privée.

D'une part, les mesures de distanciation physique nécessaires dans un contexte de crise sanitaire ont conduit à une augmentation de l'utilisation des technologies de communication à distance, modifiant la façon dont les individus utilisent les ressources numériques sur le lieu de travail, dans l'éducation ou encore dans leur vie personnelle et sociale. Ainsi, dans le milieu de travail, de nombreux employés ont été contraints de travailler à distance avec les risques que cela emporte tant d'un point de vue de la surveillance des salariés que pour la sécurité et la confidentialité des entreprises qui y recourent. Autre illustration, de nombreux dispositifs de surveillance sont également utilisés dans le secteur de l'éducation, faisant ainsi peser des risques sur les droits et libertés des étudiants et des enseignants qui les encadrent. Plus généralement, il convient de relever que la réflexion sur l'exercice des libertés « numériques » dans ce contexte doit être aussi conduite au regard des restrictions extrêmement importantes qui ont été portées aux libertés « physiques », et notamment à la liberté d'aller et venir.

D'autre part, les États ont tenté de répondre à la crise en utilisant des solutions basées sur les données pour essayer d'arrêter ou de ralentir la propagation du nouveau coronavirus. Les données sont un instrument central de mise en visibilité du virus et de sa propagation. De la donnée de santé du dépistage d'un individu aux nombres agrégés de cas présentés chaque jour par la Direction générale de la santé, jusqu'aux instruments de traçage des populations porteuses du virus et à risque : toutes ces données, personnelles ou anonymisées, visent à mettre en œuvre des soins et des politiques adaptées.

Les données sont ainsi à la fois une technologie cognitive de mise en visibilité et une ressource pour l'action publique. Dans un tel contexte, la CNIL a cherché à concilier la protection des données à caractère personnel et des libertés, dont elle est garante, et la protection de la santé qui sont toutes deux des objectifs à valeur constitutionnelle.

Avec ce rapport, la CNIL propose donc de faire un point d'étape, d'une part, sur ses activités en cette période exceptionnelle (Partie 1) avant de revenir sur les enjeux posés par l'exploitation des données à caractère personnel, exacerbés par la crise sanitaire (Partie 2)[1].

[1] Toutefois, la présente communication ne reviendra pas sur les dispositifs de traçage des contacts (manuel et numérique) mis en œuvre par le gouvernement qui ont récemment fait l'objet d'un avis trimestriel adressé au Parlement (Voir délibération n° 2020-087 du 10 septembre 2020 portant avis public sur les conditions de mise en œuvre des systèmes d'information développés aux fins de lutter contre la propagation de l'épidémie de COVID-19 (mai à août 2020)).

PARTIE 1 - Le rôle de la CNIL en temps de crise

La crise du COVID-19 a montré toute la pertinence des diverses missions du régulateur : de l'accompagnement juridique et technique *a priori* au contrôle *a posteriori,* toutes les activités de la CNIL ont fortement été mobilisées.

Au milieu des préoccupations croissantes concernant la façon dont les acteurs, privés comme publics, traitent les données à caractère personnel de leurs usagers, la CNIL a dû faire face à de nombreuses questions, parfois inédites en termes de protection de la vie privée. En s'appuyant sur un cadre et des principes qui ont montré leur robustesse en temps de crise (A) et avec réactivité (B) la CNIL a su rester à l'écoute de ses divers publics, priorisant ses actions en interne (C) sans mettre de côté son investissement au sein du collectif européen afin de contribuer à une approche harmonisée des sujets que la crise sanitaire aura fait naître (D).

A. Un cadre juridique robuste qui fonctionne en temps de crise

- **Les principes de protection des données constituent un élément essentiel de la confiance dans les traitements de données, en particulier dans les situations d'urgence**

Alors que le pays affronte la pire crise de son histoire depuis plusieurs décennies, **une leçon à tirer de cette période est la grande robustesse des principes posés par la règlementation relative à la protection des données à caractère personnel.**

La crise a révélé la pertinence de l'application de plusieurs principes de la règlementation : les notions de proportionnalité (existe-t-il un moyen moins intrusif ?) et de nécessité (quelle utilité sanitaire ?) ont été au cœur des débats ; le principe de minimisation des données permet de s'assurer que seules les données nécessaires à la gestion de la crise seront collectées alors que le principe de finalité et de limitation de la conservation des données permet d'encadrer les usages de ces données afin d'éviter tout éventuel détournement de finalités. Par ailleurs, la crise sanitaire a particulièrement bien montré l'intérêt des approches de protection des données dès la conception et de protection des données par défaut, consacrés par le RPGD, que les porteurs de projet, publics ou privés se sont efforcés d'intégrer.

Ainsi, il n'a jamais été question, dans le débat public, de lever la protection de ces droits fondamentaux ni de contourner la CNIL. Celle-ci, au contraire, a été désignée dans de nombreuses arènes comme un acteur essentiel de la définition des équilibres à atteindre dans la multitude de dispositifs et de politiques publiques nouvellement mis en place. Dans certains cas, les principes défendus par la CNIL ont même été soutenus tant par d'autres acteurs institutionnels majeurs (Défenseur des droits, Conseil national du numérique, etc.) que par le Conseil d'Etat (s'agissant notamment des caméras thermiques ou encore du recours aux drones).

- **Le principe de responsabilisation des acteurs doit être soutenu par un accompagnement du régulateur**

Le rôle de la CNIL comme « guide » des administrations et entreprises privées est apparu essentiel pour aider les pouvoirs publics et les acteurs privés à hiérarchiser les actions prioritaires. Pour être pleinement efficace, il ne s'agit pas uniquement de rappeler la loi et de la décliner à certains cas d'usage mais aussi d'affirmer une position nette sur certains projets, soit pour les soutenir (par exemple pour certaines recherches liées à la COVID-19) soit pour les dissuader (diverses applications fantaisistes notamment).

Afin de fonder ces décisions, notamment sur la nécessité et la proportionnalité, la CNIL a pu s'appuyer sur les priorités de la stratégie sanitaire définie par les autorités en lien avec le conseil scientifique, afin d'autoriser certains traitements et à l'inverse d'en décourager d'autres. Cet exemple illustre le fait que la mission de conseil de la CNIL doit pouvoir se reposer sur des expertises externes à l'activité de la Commission lorsqu'elle est confrontée à des enjeux nouveaux.

Cependant, la multiplication des initiatives en réponse à la crise a révélé les limites du principe de responsabilisation des acteurs ou, à tout le moins, a démontré que la mise en œuvre de dispositifs innovants (y compris les usages nouveaux de dispositifs préexistants) devait s'appuyer sur un accompagnement, le plus en amont possible, de la part du régulateur. En effet, ont été identifiées *a posteriori* de leurs premières utilisations, des problématiques structurantes liées à certaines solutions, notamment développées par des acteurs privés afin d'apporter leur contribution à la lutte contre la propagation du COVID-19 (par exemple, les caméras de détection du port du masque). Cet état de fait a conduit, dans certains cas, à la suspension d'expérimentations ou à une remise en cause de l'activité du fournisseur de technologie. **Cela témoigne donc de l'utilité de la démarche de la CNIL et de la nécessité, pour celle-ci, de communiquer de manière régulière sur sa doctrine afin que les acteurs puissent s'en saisir le plus en amont possible dans le cadre de leurs projets.**

Les applications de suivi des contacts : un exemple d'approche proactive de la CNIL

Face au développement d'applications automatisées de suivi des contacts dans le monde, la CNIL s'est penchée très tôt sur le sujet afin d'analyser tant juridiquement que techniquement les implications de tels dispositifs sur les droits et libertés des personnes.

Cela lui aura permis, très rapidement, de travailler à l'élaboration d'exigences communes pour ce type de dispositif avec ses homologues européens.

Dans ce contexte, le comité européen à la protection des données (CEPD) a publié, le 21 avril 2020, des lignes directrices relatives à l'utilisation de données de géolocalisation et d'outils de « suivi des contacts » dans le cadre de la pandémie de COVID-19. Cela a permis à la CNIL d'accompagner, efficacement et avec réactivité, le gouvernement dans le cadre des saisines sur l'application « StopCovid ».

B. Une organisation adaptée et une réactivité à la hauteur des enjeux de la crise sanitaire, malgré de fortes contraintes

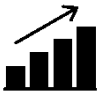
1. Les relations avec la CNIL pendant l'état d'urgence sanitaire

En cette période de crise, la CNIL a traité, en priorité, les dossiers en lien avec l'épidémie de COVID-19, la contraignant parfois à retarder d'autres actions. Son organisation a néanmoins permis de minimiser le ralentissement de ses activités. La plupart des délais accordés à ses usagers pour répondre à ses demandes ou décisions ont naturellement été allongées afin de tenir compte de ce contexte exceptionnel, conformément à ce que prévoit l'ordonnance n° 2020-306 du 25 mars 2020[2] pour certaines procédures mises en œuvre par la CNIL.

[2] Ordonnance n° 2020-306 du 25 mars 2020 relative à la prorogation des délais échus pendant la période d'urgence sanitaire et à l'adaptation des procédures pendant cette même période [en ligne]. https://www.legifrance.gouv.fr/loda/id/LEGITEXT000041756550/2020-04-17/

Evolution des modalités de saisine de la CNIL

Baisse importante des courriers postaux et appels téléphoniques



Augmentation notable des échanges électroniques (téléservices, courriels, etc.)

Mise en place d'un numéro d'urgence

A titre général, s'agissant des activités de la CNIL prises dans leur ensemble, les délais de traitement des dossiers n'ont pas été substantiellement affectés par la crise sanitaire. Des mesures d'organisation et de fonctionnement interne des services comme du Collège ont en effet été prises afin de minimiser l'impact de la crise sanitaire sur ses activités. Cette stabilité cache néanmoins quelques variations :

- Les contrôles, réalisés à titre principal sur place, de même que les vérifications en matière de droits d'accès indirect aux fichiers de sécurité publique, n'ont pas pu être réalisées du fait du confinement.
- De même, les demandes faites aux organismes dans le cadre de l'instruction des plaintes et réclamations reçues ont été, sur décision de la CNIL et sauf urgence (lorsqu'elles portent par exemple sur des dispositifs mis en œuvre dans le cadre de la gestion de la crise), suspendues, afin de ne pas faire peser de charges trop lourdes aux organismes en cette période.
- Enfin, certaines saisines traditionnelles adressées par les usagers professionnels (demande d'avis sur des projets de texte, instruction de demandes de certification, BCR, etc.), dès lors qu'elles n'étaient pas en lien direct ou indirect avec la crise sanitaire, ont pu connaître un léger décalage de traitement, principalement dû aux urgences s'intercalant dans les circuits traditionnels.

2. Une priorisation des dossiers en lien avec l'urgence sanitaire

La réactivité de la CNIL dans un contexte sanitaire exceptionnel a été mise à l'épreuve. Dès le début de la crise sanitaire la CNIL s'est organisée pour s'assurer que toutes les saisines en lien direct avec celle-ci soient traitées de manière prioritaire, parfois en urgence, avec des délais drastiquement raccourcis.

En premier lieu, **la CNIL a accompagné, à de nombreuses reprises, les pouvoirs publics dans la mise en œuvre de divers dispositifs destinés à lutter contre l'épidémie de la COVID-19 en rendant plusieurs avis**, en urgence, sur les projets de textes encadrant des traitements tels que l'application « StopCovid » ou encore les systèmes d'information nationaux « SI- DEP » et « CONTACT COVID ».

Les activités de la CNIL entre mars et juin en quelques chiffres

13 séances plénières en lien avec l'épidémie de COVID-19 dont 4 séances exceptionnelles

6 avis rendus en lien avec l'épidémie de COVID-19

En deuxième lieu, **la CNIL a intensifié les relations qu'elle entretient de façon régulière avec le Parlement au titre de sa mission d'accompagnement des pouvoirs publics.** Par la voix de sa Présidente, elle a ainsi répondu aux nombreuses sollicitations de ce dernier (cinq auditions entre avril et mai 2020) dans des délais particulièrement courts, compte tenu du calendrier d'adoption des projets de loi. Par ailleurs, les avis rendus par la Commission dans ce contexte d'urgence sanitaire ont pu contribuer utilement aux débats parlementaires autour des enjeux fondamentaux liés au respect de la vie privée et des données à caractère personnel.

En troisième lieu**, la CNIL s'est mobilisée pour instruire en priorité, dans des délais extrêmement courts, les demandes d'autorisation déposées dans le secteur de la recherche en santé et portant sur la COVID-19**[3] : 80 demandes d'autorisation ont été déposées entre mars et octobre 2020 sur ce sujet particulier sur un total de 410 demandes d'autorisation « recherche », entre janvier et octobre 2020. La CNIL a respecté des délais d'examen particulièrement courts, parfois en quelques heures (grâce aux échanges préalables ayant pu intervenir avec le responsable de traitement) des demandes d'autorisation en matière de recherche médicale, déposées par exemple par l'INSERM ou l'AP-HP.

Enfin, si certains contrôles, réalisés à titre principal sur place, ont dû être reportés et l'instruction classique de certaines plaintes suspendue afin de tenir compte du contexte de crise (cf. supra), **les investigations ayant trait aux divers dispositifs mis en œuvre dans le cadre du COVID-19 ont été priorisées, attestant ainsi de la mobilisation de l'ensemble des activités de la CNIL.**

C. Un régulateur à l'écoute de ses divers publics

La CNIL offre, depuis de nombreuses années, de multiples canaux permettant aux particuliers comme aux professionnels de faire part de leurs interrogations (voire de leurs inquiétudes) en matière de protection des données à caractère personnel. A l'écoute de ses divers publics (particuliers, organismes privés et publics, associations, etc.), la CNIL a également su prioriser ses actions en fonction des principales préoccupations de ces derniers qu'il s'agisse de son activité d'accompagnement (1) ou de son activité répressive (2).

1. Un accompagnement au plus près des préoccupations actuelles

Si le volume de saisines reçues par la CNIL est resté stable (de manière globale), les thèmes faisant l'objet de saisines de la CNIL et les acteurs à l'origine de celles-ci ont fortement évolué. A titre général, les saisines en lien avec la crise sanitaire, soit très directement (dispositifs publics de gestion de la crise, par exemple) soit plus indirectement du fait du confinement puis du déconfinement (en matière de télétravail, d'utilisation de la visioconférence, d'examens à distance, de délivrance de masques, de contrôle du bon respect des règles, etc.) ont été très importantes. La CNIL a publié de nombreuses fiches et conseils pratiques à destination des divers publics de la CNIL.
En effet, les mesures relatives à la crise de la COVID-19 ont un effet considérable sur le quotidien numérique des citoyens et résidents français (voir infra, « *Une intensification des pratiques numériques quotidiennes* »). Aussi, la CNIL a mis à la disposition du public des fiches et conseils pratiques à destination essentiellement :

- **du grand public,** notamment dans le cadre de l'utilisation d'outils de visioconférence[4] ;

[3] Recherches sur la COVID-19 : la CNIL se mobilise. CNIL, 26 mars 2020. https://www.cnil.fr/fr/recherches-sur-le-covid-19-la-cnil-se-mobilise
[4] COVID-19 : les conseils de la CNIL pour utiliser les outils de visioconférence. CNIL, 9 avril 2020. https://www.cnil.fr/fr/covid-19-les-conseils-de-la-cnil-pour-utiliser-les-outils-de-visioconference

- **des salariés** qui ont recours à des solutions de télétravail afin de leur faire part des bonnes pratiques à suivre et des règles pour garantir leur sécurité et celle de leur entreprise.
- **des employeurs** afin de les aider à sécuriser les données à caractère personnel de leurs employés durant cette transition.
- **de la communauté enseignante** dans leurs efforts de mise en place d'une continuité pédagogique.

De plus, les diverses sollicitations dont la CNIL a été destinataire (à travers, notamment, les demandes de conseil) durant cette période ont permis de soulever de nouvelles problématiques sur lesquelles la CNIL a dû rapidement apporter des éléments de réponse. **La crise sanitaire aura ainsi permis l'élaboration de points doctrinaux structurants sur des problématiques diverses :**

- Les employeurs, syndicats et organisations professionnelles ont saisi la CNIL de nombreuses demandes dans le cadre du confinement puis du déconfinement relatives à des dispositifs de lutte contre l'épidémie dans le cadre du travail : mise en œuvre de dispositifs de contrôle de température, remontée d'informations sur les salariés malades, etc.
- La CNIL a également été sollicitée par les communes et d'autres collectivités territoriales sur les dispositifs mis en œuvre ou envisagés dans le cadre de la gestion de la crise sanitaire, tels que, par exemple, les conditions d'utilisation de fichiers à des fins de distribution de masques ou la mise en place de registres communaux d'alerte et d'information des populations.
- En se penchant très tôt sur les applications de suivi des contacts (tant d'un point de vue technologique que juridique), la CNIL a pu anticiper l'examen de l'application « StopCovid ». La CNIL a également maintenu une veille régulière des débats entre scientifiques afin de consolider ses avis et d'identifier des points de contrôle.
- Enfin, les fournisseurs de technologies et certains de leurs clients (dont notamment les sociétés de transport) ont également saisi la CNIL de sollicitations sur les dispositifs de gestion de la crise, dans le contexte du déconfinement : caméras dites « intelligentes », caméras thermiques, etc.

Enfin, la mise en place d'une page dédiée sur son site internet[5] aura permis à la CNIL de valoriser ses divers travaux et de diffuser l'ensemble de ses positions et/ou recommandations à un public le plus large possible. Pour enrichir le débat public, la CNIL a également publié sur son site de prospective « linc.cnil.fr » une série d'articles mettant en perspective les dispositifs utilisés pour gérer la crise sanitaire (voir annexe 1).

2. La priorisation des sujets COVID-19 dans les activités répressives de la CNIL

L'activité répressive de la CNIL n'a pas été en reste face aux divers enjeux que la crise sanitaire fait peser sur les droits et libertés des personnes.

❖ Les dispositifs mis en œuvre pour gérer l'épidémie au cœur des plaintes « COVID-19 »

La mise en place de dispositifs innovants de traçage des contacts, l'installation de caméras thermiques ou le recueil généralisé d'informations médicales au sein d'entreprises, l'usage de solutions de surveillance des examens à distance par exemple ont généré un certain nombre de plaintes.

Les plaintes reçues depuis mars reflètent les préoccupations générées par la mise en place de dispositifs technologiques nouveaux et spécifiques au contexte comme par la collecte de données

[5] Coronavirus (COVID-19). https://www.cnil.fr/fr/coronavirus-covid-19

découlant des mesures prises aux fins de limiter la propagation du virus. Ces plaintes portent notamment sur :

Environ 40 plaintes déposées en lien avec la COVID-19

- **la conformité des dispositifs de traçage des contacts ;**
- **la licéité de la collecte de données de santé par les employeurs, par des sociétés privées (entreprises du bâtiment, EPHAD) ou établissements publics à l'égard de leurs clients, usagers ou visiteurs** (questionnaires de santé, relevés quotidiens de températures manuels ou automatisés, etc.) ;
- **la légalité de la réutilisation de fichiers détenus par des associations de personnes vulnérables ou par les collectivités** dans le cadre de plans d'alertes ou de la distribution de masques par ces dernières ;
- **les conditions de mise en œuvre de solutions technologiques de surveillance des examens à distance ;**
- **la collecte de données jugée excessive (par les requérants) par diverses structures** (université, commune, syndicats, etc.) à des fins de récupération de masques ou la réalisation de sondages visant à savoir comment le confinement a été vécu par les étudiants.

L'instruction de ces dossiers a conduit les services de la CNIL à rappeler leurs obligations à de nombreux organismes, engagés à modifier les conditions de traitements de données ou à y mettre fin le cas échéant.

❖ L'activité de contrôle : reflet des préoccupations actuelles

En dehors des investigations menées sur les systèmes d'information mis en place par le gouvernement pour gérer la crise sanitaire (« SI-DEP », « CONTACT COVID » et l'application « StopCovid »)[6], la CNIL conduit également des investigations de dispositifs autonomes. Ces contrôles, dont certains sont encore en cours d'instructions, s'appuient sur des plaintes, des signalements reçus ou tout simplement sur l'actualité.

23 sur 160 contrôles réalisés depuis le début de l'année ont un lien, direct ou indirect, avec la crise sanitaire

Plus particulièrement, la CNIL a diligenté des contrôles auprès du ministère de l'Intérieur concernant l'usage de drones dans plusieurs villes. Ces contrôles ont visé des services de la police nationale et de la gendarmerie. Des vérifications similaires ont été effectuées auprès de plusieurs communes dont les polices municipales ont également eu recours à de tels dispositifs. Les premières demandes d'information à l'initiative de la CNIL datent du 23 avril 2020 et sont en cours d'instruction.

[6] Pour rappel, ces dispositifs ont déjà fait l'objet d'un avis trimestriel adressé au Parlement présenté à la Séance plénière du 10 septembre 2020.

D. Une activité qui s'inscrit dans un contexte européen : la CNIL au sein du CEPD

Particulièrement sollicitées par leur public, les autorités de protection des données européennes ont rapidement publié des recommandations à destination des acteurs privés comme publics. Sur certains sujets, le besoin de recommandations et d'harmonisation a rapidement été identifié et a conduit le CEPD a publié des lignes directrices (sous formes de déclarations) dans des circonstances tout à fait exceptionnelles[7].

Les activités du CEPD entre mars et juin en quelques chiffres

16 plénières relatives aux questions en lien avec l'épidémie de COVID-19

Une dizaine de courriers adoptés en réponse à des sollicitations européennes (parlementaires,

4 déclarations, 2 lignes directrices

La CNIL a ainsi participé activement à l'élaboration de plusieurs avis du collectif européen, notamment :

- sur les lignes directrices relatives à l'utilisation de données de géolocalisation et d'outils de « suivi des contacts » dans le cadre de la pandémie de COVID-19[8].
- sur les lignes directrices relatives à l'utilisation des données de santé à des fins de recherche scientifique et celles relative aux traitements de données personnelles mis en œuvre dans le cadre de la réouverture progressive des frontières au sein de l'Union.

Par ailleurs, la crise sanitaire actuelle aura conduit à l'intensification des échanges quotidiens de la CNIL avec ses homologues européens au sein du CEPD. En effet, la désignation de « points de contacts » au sein de chaque autorité et la mise à disposition d'un espace collaboratif en ligne dédié aux sujets relatifs au COVID-19[9] aura permis de faciliter les échanges que la CNIL a pu avoir avec ses homologues européens. **Ces derniers ont permis d'éclairer les réflexions et travaux de la CNIL sur divers sujets** (traçage des contacts, caméras dites « intelligentes », données de localisation) **afin d'assurer, au mieux, une approche harmonisée des régulateurs face à des questions, souvent inédites, que conciliation entre protection de la santé et protection de la vie privée suscite.**

[7] Certaines lignes directrices ont été élaborées en quelques semaines, fruit d'un travail intense entre les différentes autorités de protection des données.
[8] Lignes directrices 4/2020 relatives à l'utilisation de données de localisation et d'outils de recherche de contacts dans le cadre de la pandémie de COVID-19. CEPD, 21 avril 2020. https://edpb.europa.eu/our-work-tools/our-documents/linee-guida/guidelines-042020-use-location-data-and-contact-tracing_fr
[9] Le secrétariat du CEPD a créé un espace dédié sur la plate-forme Confluence (plate-forme d'échange d'informations du CEPD) pour faciliter l'échange bilatéral et multilatéral d'informations entre les membres du CEPD.

PARTIE 2 - Les enjeux posés par l'utilisation des données à caractère personnel dans le contexte du covid-19 : constats et perspectives

2.1 - Une intensification des pratiques numériques quotidiennes[10]

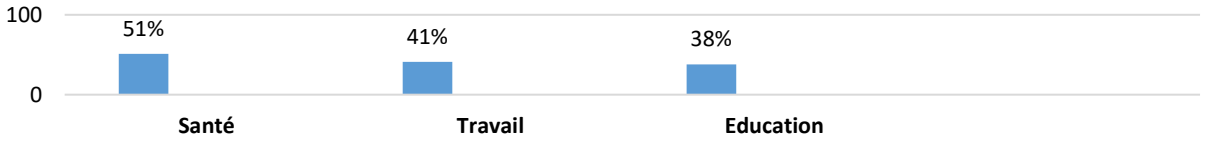
L'épidémie du Covid-19 et les mesures de confinement et de distanciation sociale imposées à la population ont fait évoluer massivement les pratiques numériques. Selon les enquêtes de Médiamétrie, le temps passé sur Internet a cru de plus de 36 % durant la seconde quinzaine de mars 2020 par rapport à l'année précédente. L'utilisation des services numériques habituels s'est intensifiée. Les réseaux sociaux ont été utilisés massivement pour garder le lien entre famille, amis et collègues. Les sites des médias ont connu des chiffres de fréquentation en forte hausse, tout comme les plateformes de streaming vidéo (Youtube, Netflix, etc.) ou les sites de e-commerce (Amazon, Fnac, etc.) et de livraisons de courses ou de repas. Des petits commerçants ont également été contraints de se lancer dans le commerce en ligne ou à distance pour poursuivre leur activité. Ce déploiement rapide et non anticipé vers des solutions technologiques plus ou moins maîtrisées fait craindre des défauts de conformité vis-à-vis de la collecte et du traitement de données personnelles.

58 %

des personnes interrogées ont utilisé au moins une solution de visioconférence pour un usage personnel pendant le confinement.

Des pratiques jusqu'ici marginales ou minoritaires – télétravail, télémédecine, téléenseignement – auront connu à l'occasion du confinement une adoption et une intensification particulièrement fortes, s'introduisant ainsi dans la vie quotidienne des utilisateurs. Cette diffusion a également été un révélateur des inégalités sociales face au numérique.

Pendant la crise, avez-vous eu recours à des outils numériques ?
Pourcentage des personnes ayant répondu "OUI", par usage



A. Un basculement rapide vers le télétravail

Le télétravail est devenu en l'espace de quelques semaines la norme pour plus d'un tiers des personnes en emploi[11]. L'essor massif des outils de travail à distance en témoigne. Plus de 7000 clients payants

[10] Les chiffres et graphiques présentés dans cette section sont issus d'un sondage IFOP réalisé en ligne, du 25 août au 31 août 2020, auprès d'un échantillon de 1 001 personnes, représentatif de la population française âgée de 18 ans et plus.

[11] Selon l'INSEE, 34 % des personnes en emploi ont télétravaillé durant le confinement sanitaire, 35 % ont continué à se rendre sur le lieu de travail et un tiers ont subi une restriction d'activités. Le recours au télétravail est fortement lié à la catégorie sociale. 58 % des cadres et professions intermédiaires ont télétravaillé, contre 20 % des employés et 2 % des

se sont inscrits sur Slack en mars 2020 (contre 5 000 au cours du trimestre précédent). Zoom a vu son chiffre d'affaires augmenter de 78 % au-delà de ses estimations. Fin février, l'entreprise comptait 2,2 millions d'utilisateurs supplémentaires, soit plus que toute l'année précédente. Entre le 11 et le 19 mars, le nombre d'utilisateurs de Microsoft Teams s'est accru de 12 millions pour atteindre 44 millions d'utilisateurs au total.

L'absence d'anticipation des modalités de travail à distance au sein des entreprises et des institutions publiques les a conduits à recourir à des solutions proposées par des acteurs de marché, pour l'essentiel états-uniens. Parmi les outils les plus plébiscités, et en même temps décriés pour ses failles de sécurité, l'application Zoom a par exemple été utilisée par les parlementaires pour des auditions et réunions de travail. En outre, des salariés ont été contraints d'utiliser leurs ordinateurs et téléphones personnels pour exercer leur activité professionnelle à distance, soulevant des risques en matière de sécurité des données. Ces exemples témoignent de l'importance de l'anticipation dans la prise en compte, pour l'ensemble des organismes, des enjeux de sécurité des données à caractère personnel.

Face à un tel constat, des recommandations[12] ont été publiées sur le site web de la CNIL pour aider à la bonne sécurisation des données durant cette période particulière. Alors que le recours au télétravail s'installe de façon durable dans le quotidien de nombreux français, la CNIL appelle les responsables de traitement à sécuriser les dispositifs parfois mis en place dans l'urgence afin d'offrir des conditions de travail pérennes permettant de traiter des données personnelles dans de bonnes conditions.

Le télétravail : vecteur de violations de données ?

De nombreuses notifications de violations de données, reçues durant le confinement, sont directement liées à une mauvaise gestion des outils permettant le télétravail. Le recours massif au télétravail, dans l'urgence, a parfois contribué à fragiliser les systèmes d'information des organismes. En particulier, cela a pu engendrer des mauvaises pratiques qui ont favorisé les attaques par rançongiciels[13] et par hameçonnage[14] :

- des mauvaises configurations des outils de sécurité (mise en place d'un réseau privé virtuel (VPN) mal configuré ou dont les correctifs de sécurité n'ont pas été correctement appliqués ou bien un mauvais paramétrage des contrôles d'accès) ;
- un assouplissement des mesures de sécurité (par exemple, une politique de changement de mots de passe affaiblie ou un contournement de la restriction des adresses IP pour permettre le travail à distance).

Par ailleurs, le télétravail a engendré une explosion des transmissions de données par mail, entrainant dès lors une augmentation significative de divulgations non autorisées de données.

De même, la situation a facilité les tentatives d'attaque au cours desquelles un tiers non autorisé contacte un organisme en se faisant passer pour un collaborateur distant ayant besoin d'accéder à une ressource de l'entreprise.

ouvriers. À l'inverse, les personnes les plus modestes ont davantage continué à aller travailler sur site. Ce fut en particulier le cas des ouvriers (53 %), devant les employés (41 %), agriculteurs, chefs d'entreprise et indépendants (40 %), les cadres et professions intermédiaires étant nettement en retrait (21 %). https://www.insee.fr/fr/statistiques/4513259

[12] Les conseils de la CNIL pour mettre en place du télétravail. CNIL, 12 mai 2020. https://www.cnil.fr/fr/les-conseils-de-la-cnil-pour-mettre-en-place-du-teletravail

[13] Technique d'attaque courante de la cybercriminalité, le rançongiciel ou ransomware consiste en l'envoi à la victime d'un logiciel malveillant qui chiffre l'ensemble de ses données et lui demande une rançon en échange du mot de passe de déchiffrement (Source : ANSSI).

[14] Ce type d'attaque vise à obtenir du destinataire d'un courriel d'apparence légitime qu'il transmette ses coordonnées bancaires ou ses identifiants de connexion à des services financiers, afin de lui dérober de l'argent. L'hameçonnage peut également être utilisé dans des attaques plus ciblées pour essayer d'obtenir d'un employé ses identifiants d'accès aux réseaux professionnels auxquels il peut avoir accès (Source : ANSSI).

Enfin, le télétravail a pu complexifier la fluidité des échanges entre collaborateurs en cas de violation de données notamment pour identifier l'origine de l'incident de sécurité, pour documenter de façon adéquate la violation, pour restaurer rapidement les systèmes compromis et pour, le cas échéant, notifier la violation à la CNIL dans les délais impartis.

❖ **Des nouvelles formes de surveillance au travail**

Les enjeux de sécurité ne sont par ailleurs pas les seuls soulevés par le recours massif au télétravail.

Dans le secteur professionnel, un autre enjeu majeur concerne les dispositifs de surveillance de l'activité des salariés en télétravail. Celle-ci, qui est traditionnellement un des motifs principaux de plaintes et appels reçus par la CNIL, s'est appuyée sur une myriade de dispositifs, dont certains illicites, visant à contrôler à distance le travail des salariés (keylogger, demande de laisser la webcam allumée en permanence, etc.).

26 %

des personnes interrogées ayant pratiqué le télétravail,
affirment avoir eu le sentiment d'avoir été davantage
surveillé que d'habitude par leur employeur.

Alors que le recours au travail à distance semble amené à se poursuivre dans les prochains mois, la CNIL reste particulièrement vigilante sur l'usage de ces dispositifs technologiques qui traduisent de nouvelles formes de management. L'autonomie accrue accordée aux salariés s'accompagne de nouvelles pratiques de contrôle de leur activité qui, sans préjuger de leur conformité au RGPD, restent également génératrices d'un sentiment de surveillance pour les salariés.

air2020 : un évènement dédié au thème numérique et travail

Lors d'un colloque de réflexion éthique organisé le 9 novembre (Évènement air2020)[15], la CNIL s'est penchée sur les nouveaux rapports qui lient le travail aux technologies afin d'en saisir les logiques et les enjeux.

B. Des pratiques d'enseignement à distance désordonnées

Les plateformes d'enseignement à distance (e-learning) ont connu un succès important en raison de la fermeture des écoles et du plan de continuité pédagogique. Le ministère de l'Éducation nationale préconisait en mars 2020 l'usage pour l'enseignement à distance des outils « Ma classe à la maison », proposé par le CNED, et les ENT (environnement numérique de travail), ou le logiciel de gestion de vie scolaire Pronote.

Cependant, la rapidité de l'annonce de la fermeture des écoles par le chef de l'État le 12 mars n'a pas permis aux équipes enseignantes d'anticiper la prise en main de ces outils par les professeurs, les élèves et les parents. Face aux problèmes techniques de Pronote, à la saturation de la plateforme du CNED et surtout à la maîtrise inégale de ces environnements numériques, nombre d'enseignants ont préféré recourir aux outils utilisés quotidiennement par leurs élèves : WhatsApp, Discord, Snapchat, etc. Ces services ont en outre l'avantage de fonctionner de manière fluide sur smartphone, souvent le seul équipement numérique présent dans les foyers en l'absence d'ordinateur. Soumis à des

[15] Évènement air2020 : quelles mutations dans le monde du travail ? CNIL, 23 septembre 2020. https://www.cnil.fr/fr/evenement-air2020-quelles-mutations-dans-le-monde-du-travail

injonctions contradictoires, les équipes éducatives ont tenté de mettre en place des solutions palliatives au détriment, parfois, du respect du RGPD.

De même, la mise en place d'un service d'enseignement à distance au sein des établissements d'enseignement supérieur a conduit à l'utilisation de dispositifs parfois peu respectueux des droits des individus en matière de protection des données personnelles. Les examens de fin d'année ont en particulier retenu l'attention, du fait des modalités de télésurveillance envisagées par certains établissements pour l'organisation d'examens à distance : vidéo continue, prise de photographies aléatoires, prise à distance du contrôle de l'ordinateur de l'étudiant, algorithmes de détection de la fraude, etc. Cette inquiétude s'est traduite par la réception par la CNIL de plusieurs appels et plaintes sur le sujet de la télésurveillance et la publication d'un article sur les « rappels et conseils » de la CNIL sur la mise en œuvre de tels dispositifs[16].

C. L'explosion des pratiques de la médecine à distance

Jusqu'alors marginale, la médecine à distance a connu un essor spectaculaire. Ceci s'explique notamment par l'impulsion des plateformes numériques telles que Doctolib qui offrait son service de téléconsultations aux médecins abonnés le temps de la crise[17] et par l'annonce faite par le gouvernement dès la mi-mars d'une prise en charge à 100 % par l'assurance maladie de la téléconsultation ainsi que la possibilité d'y recourir avec un autre médecin que son médecin habituel. Plus d'un million de téléconsultations ont été facturées entre le 6 et le 12 avril selon l'Assurance-maladie (soit 28 % de l'ensemble des consultations contre 0,1 % entre le 2 et le 8 mars). En 2019, le total des téléconsultations était d'à peine 60 000.

Cet essor des services de médecine à distance soulève des enjeux en matière de centralisation de données de santé par des acteurs privés et des risques inhérents en matière de sécurité de ces dernières. À ce titre, la CNIL a reçu en juillet une notification d'une entreprise de prise de rendez-vous en ligne indiquant qu'elle avait subi une attaque informatique ayant permis à l'attaquant d'accéder à environ 6 000 rendez-vous de patients.

D. Une intensification des pratiques qui met en lumière les inégalités numériques

Dans l'ensemble de nos sphères sociales (professionnelles, éducatives, personnelles, loisirs, etc.), l'utilisation de services à distance s'est intensifiée. Il est encore tôt pour déterminer si cette intensification de nos pratiques numériques mènera à un changement d'habitude durable. Quoi qu'il en soit, elle révèle de profondes inégalités sociales quant à l'accès numériques. Pour les 12 % de français ne disposant pas de connexion à Internet[18], les mesures de confinement ont accentué l'exclusion sociale. En outre, nombre de foyers ne disposent pas du matériel ou d'un débit de connexion adéquat. Des familles ont par exemple été contraintes de se partager un unique smartphone pour assurer toutes leurs pratiques numériques, du suivi des cours à distance donnés par les professeurs au maintien d'un lien social via les réseaux sociaux. Outre les difficultés pratiques et le retard scolaire que cela implique, ce partage familial d'un même dispositif pose questions en termes

[16] Surveillance des examens en ligne : les rappels et conseils de la CNIL. CNIL, le 20 mai 2020. https://www.cnil.fr/fr/surveillance-des-examens-en-ligne-les-rappels-et-conseils-de-la-cnil

[17] Le ministère de la Santé a publié sur son site la liste des outils numériques de médecine à distance respectant un certain nombre de prérequis. https://solidarites-sante.gouv.fr/soins-et-maladies/maladies/maladies-infectieuses/coronavirus/professionnels-de-sante/article/teleconsultation-et-covid-19-qui-peut-pratiquer-a-distance-et-comment

[18] INSEE, Enquête annuelle auprès des ménages sur les technologies de l'information et de la communication (TIC ménages), octobre 2019, https://www.insee.fr/fr/statistiques/fichier/version-html/4241397/ip1780.pdf

de confidentialité des informations de chacun des utilisateurs. Par ailleurs, pour les 13 millions de Français en difficulté avec les outils numériques, la numérisation de nombreux services (de l'obtention d'une attestation de déplacement à la réalisation de démarches administratives) a accru les inégalités d'usage entre les individus.

A ce titre, les appels reçus par la CNIL témoignent de la détresse d'une partie de la population face à ces technologies numériques qu'ils ne maîtrisent pas. Pour certains d'entre eux, la CNIL est perçue comme l'institution pouvant résoudre leurs problèmes liés au numérique même si ceux-ci ne relèvent pas de la collecte ou du traitement de leurs données à caractère personnel. Autre indicateur de ce désarroi, la plateforme « Solidarité numérique »[19] mise en place à la mi-mars par la MedNum, coopérative des acteurs de la médiation numérique, a reçu en moyenne 350 appels par jour entre l'ouverture du centre d'appel téléphonique et l'été.

Enfin, les pratiques numériques en période de confinement ont conduit à un glissement des frontières entre nos différentes sphères sociales (vie domestique, vie privée, vie professionnelle). Les pratiques liées au télétravail ont par exemple fait entrer le domicile des individus dans leur sphère professionnelle. Cette recomposition des frontières sociales a donné lieu à un certain nombre de troubles et a pu faire l'objet de conflits ou de négociations, entre les individus et les organisations, qui conduisent à questionner les valeurs accordées à la vie privée. Les individus ont mis en place des stratégies et développées des compétences pour gérer les frontières entre leurs sphères sociales, du refus de l'usage de la webcam à la mise en scène d'un arrière-plan. L'intensification des pratiques numériques laissent à penser que le confinement a pu être un moment de conversion numérique, entendu comme une période qui conduit à interroger la place du numérique dans nos vies.

2.2 - Les dispositifs de surveillance mobilisés pour gérer l'épidémie

Les dispositifs de surveillance mobilisés pour gérer l'épidémie soulèvent une deuxième série d'enjeux en termes de protection des données. En effet, les données à caractère personnel sont vues comme une ressource pour répondre rapidement et efficacement aux défis sanitaires (surveillance du respect des mesures sanitaires, accompagnement des stratégies de confinement et/ou de déconfinement au moyen d'outils numériques, protection des personnes vulnérables, etc.).

A. Une exploitation des données pour lutter contre la propagation du virus et/ou accompagner les publics fragiles

Cette crise a conduit les acteurs tant publics que privés à réfléchir à de nouveaux usages des données. Par ailleurs, la crise sanitaire a conduit les autorités publiques, les institutions académiques et les chercheurs à accroitre leur demande de partage de données auprès des entreprises.

1. Les données de santé, une ressource essentielle

❖ **Dans le secteur de la santé**

- **La recherche dans le domaine de la santé :** afin de lutter contre l'épidémie et de trouver des solutions thérapeutiques efficaces, dans l'attente de la découverte d'un vaccin, de nombreux projets de recherches ont été mis en œuvre. Recherches impliquant la personne humaine ou recherches portant uniquement sur des données, l'ensemble des projets

[19] https://solidarite-numerique.fr/

impliquant le traitement de données de patients pris en charge en France a, théoriquement[20], été mis en œuvre après la réalisation de formalités auprès de la CNIL ou de mise en conformité avec une méthodologie de référence. **La multiplication des projets de recherche soulève la question de la fiabilité et de l'exploitabilité des résultats de ces études, qui portent sur des nombres assez réduits de patients dans le cadre d'approches souvent similaires. Ce constat soulève ainsi des interrogations en matière de méthodologie et d'éthique.**

- **La nécessaire centralisation de données au niveau national :** la crise sanitaire a été l'occasion, pour les pouvoirs publics, d'éprouver les systèmes existants de remontées d'informations. La nécessité de disposer, au niveau national, de chiffres frais et fiables, afin de coordonner la politique sanitaire globale et également d'informer, s'est avérée prégnante. Afin de répondre aux besoins, plusieurs systèmes d'information (« SIDEP » et « Contact COVID ») ont été créés, en plus des outils existants (tels que SIVIC par exemple) spécifiquement dans le cadre de la lutte contre l'épidémie. La CNIL a eu l'occasion de se prononcer à plusieurs reprises sur ces outils préalablement à leur mise en œuvre et continuera à se prononcer sur ces outils, en tant que de besoin.
- **La montée en puissance du « Health Data Hub » (Plateforme des données de santé – PDS)** : la crise sanitaire a accéléré le démarrage de la plateforme technologique de la PDS en l'autorisant, par arrêté, à centraliser les données du SNDS pour les besoins de la recherche sur la Covid-19. Lors de son avis du 20 avril 2020, la CNIL s'était inquiétée, d'une part, de cette mise en place anticipée nécessitant des opérations techniques structurantes et, d'autre part, du prestataire d'hébergement informatique (Microsoft) impliquant de potentiels transferts de données aux Etats-Unis et un accès direct par les autorités américaines. Cet hébergement, vivement contesté, prend aujourd'hui une dimension particulière depuis la décision « Schrems II » de la Cour de justice de l'Union européenne[21]. Le Conseil d'Etat a d'ailleurs eu à se prononcer à nouveau en octobre 2020 sur cette question lors d'un recours en référé relatif à la solution technologique de la PDS. La CNIL restera vigilante sur les projets qui seront mis en œuvre au sein de cette solution technologique.

❖ L'usage des données de santé par les employeurs et les structures sportives

La perspective d'une phase de « déconfinement » a conduit tant les particuliers que les professionnels à s'interroger sur les mesures à mettre en œuvre aux fins de limiter la propagation du virus et d'assurer en toute sécurité la reprise de l'activité.
Plusieurs organismes ont ainsi conditionné l'accès à un lieu ou à un service au renseignement d'informations sur l'état de santé de leurs salariés. La CNIL a reçu plusieurs demandes d'information et plaintes relatives à la remontée de données de santé relatives aux employés via notamment la mise en place systématique de questionnaires de santé.

Ce sujet a rapidement fait l'objet de publications sur le site web de la CNIL ; celles-ci ont été mises à jour à plusieurs reprises afin de tenir compte des questions récurrentes reçues par les différents services, y compris s'agissant du déploiement de solutions logicielles envisagées pour faciliter la gestion par les employeurs de la crise sanitaire.[22]

---

[20] Il a été fait écho dans les médias de nombreux projet de recherche qui n'ont pas été porté à la connaissance de la CNIL, ce qui ne préjuge pas de l'absence de conformité.
[21] CJUE, arrêt C-311/18 du 16 juillet 2020, Data Protection Commissioner contre Facebook Ireland Limited et Maximillian Schrems.http://curia.europa.eu/juris/document/document.jsf?docid=228677&mode=req&pageIndex=1&dir=&occ=first&part=1&text=&doclang=FR&cid=4532167
[22] Coronavirus (COVID-19) : les rappels de la CNIL sur la collecte de données personnelles par les employeurs. CNIL, 23 septembre 2002. https://www.cnil.fr/fr/coronavirus-covid-19-les-rappels-de-la-cnil-sur-la-collecte-de-donnees-personnelles-par-les

Au-delà de la sphère du travail, plus récemment, de multiples structures sportives (associations, clubs) se sont interrogées sur la possibilité de mettre en œuvre des mesures adaptées pour limiter la propagation du virus et assurer en toute sécurité la reprise des activités et des manifestations sportives (entraînements, tournois, rencontres amicales, etc.). Leurs interrogations, similaires à celles déjà évoquées dans le contexte employeur/employé ont porté principalement sur les conditions dans lesquelles des données à caractère personnel des sportifs, entraineurs, arbitres ou encadrants, notamment relatives à la santé peuvent être utilisées (prise systématique des températures avant d'accéder à un équipement sportif, organisation de tests virologiques préalablement à l'organisation d'une manifestation sportive, communication d'un test virologique négatif en cas d'absence du sportif à un entraînement, remplissage d'un questionnaire de santé dédié spécifiquement aux risques d'exposition à la COVID-19, etc.).

Ainsi, la CNIL a rappelé, sur son site web, les principes en matière de protection de la vie privée et des données à caractère personnel appliqués à la pratique sportive[23].

2. La réutilisation des fichiers des collectivités pour la distribution de masques et l'aide aux populations vulnérables.

En dehors du secteur de la santé et RH, les données à caractère personnel sont également vues comme des ressources permettant de contribuer à la lutte contre la COVID- 19 ; tel est le cas pour les collectivités territoriales.

Ainsi, dès le début de l'épidémie et dans une démarche proactive, la CNIL a pris contact avec les trois principaux niveaux de collectivités territoriales, représentées par Régions de France, l'Association des Départements de France (ADF) et l'Association des Maires de France (AMF) afin de faire connaitre aux élus de terrain sa mobilisation et sa disponibilité pour accompagner les initiatives des collectivités permettant de lutter contre la pandémie tout en protégeant la vie privée des personnes. A cette occasion, la CNIL a invité ces principales associations à lui transmettre toute problématique « Informatique et Libertés » se rapportant à la gestion de la crise sanitaire afin d'apporter des réponses concrètes aux collectivités. Cette démarche aura ainsi permis de porter à la connaissance de la CNIL « en temps réel » les difficultés rencontrées par les collectivités.

Appelées à jouer un rôle majeur dans la gestion de la crise sanitaire, en particulier s'agissant de la distribution de masques ou de la protection des personnes les plus vulnérables, les collectivités ont dû faire preuve de réactivité pour mener bien à leurs missions. De manière inéluctable, la question de la réutilisation des fichiers existants et détenues par elles s'est posée. Il est à noter que certains fichiers détenus par les collectivités peuvent présenter une utilité certaine dans de nombreux contextes et en particulier dans le contexte actuel de crise sanitaire dès lors qu'ils permettent de recenser une large partie de la population sur un territoire donné (ex : fichier de la taxe d'habitation, la liste électorale, etc.).

Face aux interrogations des collectivités, la CNIL a eu l'occasion d'une part, de rappeler les règles applicables à l'utilisation de certains fichiers afin de garantir un niveau de protection maximale de la vie privée des personnes concernées[24] et, d'autre part, de livrer des recommandations pragmatiques quant à la mobilisation de fichiers préexistants pour procéder aux opérations de distribution de masques, notamment sur l'utilisation du fichier de la taxe d'habitation[25].

---

[23] COVID-19 et pratiques sportives : quel cadre juridique pour la collecte de données de santé ? CNIL, 14 octobre 2020. https://www.cnil.fr/fr/covid-19-et-pratiques-sportives-quel-cadre-juridique-pour-la-collecte-de-donnees-de-sante

[24] Les registres communaux d'alerte et d'information des populations. CNIL, le 14 avril 2020. https://www.cnil.fr/fr/les-registres-communaux-dalerte-et-dinformation-des-populations

[25] La CNIL considère possible l'utilisation du fichier de la taxe d'habitation pour la distribution des masques par les collectivités territoriales. CNIL, 1 mai 2020. https://www.cnil.fr/fr/la-cnil-considere-possible-utilisation-fichier-taxe-dhabitation-pour-distribution-des-masques

Malgré cette démarche, la CNIL a néanmoins reçu quelques plaintes relatives à ces questions de réutilisations de fichiers pour lesquelles elle est intervenue pour rappeler le cadre légal.

3. L'usage des données de localisation à des fins de lutte contre la COVID-19

Le propre d'une épidémie est la circulation rapide du virus. L'un des enjeux majeurs dans la production de données dans le cadre d'une crise sanitaire réside dans la compréhension des processus de circulation du virus. Rendre visible la propagation spatiale du virus poursuit plusieurs finalités pour lesquelles le type et la granularité des données vont varier : comprendre les caractéristiques de propagation spatiale du virus (comment le virus se propage), prédire les prochaines zones touchées et anticiper la mise en œuvre de mesures sanitaires adaptées (où le virus se propage), et identifier les personnes ayant été en contact avec le virus pour permettre une mise en quarantaine anticipée et ciblée sur des populations précises (qui le virus est susceptible de contaminer).

Un partage de données « anonymisées » en Europe

L'opérateur de télécommunications Orange a annoncé partager des données de localisation « anonymisées » avec plusieurs (INSERM, préfectures, AP-HP) afin de permettre aux épidémiologistes de modéliser la propagation de la maladie.

Plus largement en Belgique, en Italie, en Autriche ou encore en Allemagne, plusieurs opérateurs de télécommunications ont déclaré avoir fourni des données « anonymisées » pour surveiller les déplacements des personnes et s'assurer du respect des mesures de confinement.

Au niveau européen, la Commission européenne a demandé aux principaux opérateurs téléphoniques de transmettre leurs données au JRC, le centre d'étude scientifique de la Commission européenne, afin d'analyser la propagation de l'épidémie.

L'épidémiologie a, depuis plus d'un siècle, construit des modèles statistiques visant à comprendre et prédire la propagation des épidémies. Les résultats issus des modèles sont dépendants des données disponibles en entrée et des hypothèses qui les nourrissent. Les déplacements de population sont une variable centrale. Or, comme l'explique au Monde Vittoria Colizza, directrice de recherches à l'Institut Pierre-Louis d'épidémiologie et de santé publique (Inserm-Sorbonne Université) : « *Dans une pandémie de ce type, il y a une forte perturbation de la mobilité : les gens s'adaptent et ne voyagent plus à cause du confinement et de la restriction des déplacements, les trains circulent moins, les vols sont annulés. Les modèles de mobilité issus de la vie normale ne sont plus applicables et auraient donné des prédictions erronées. Il est important d'informer nos modèles avec des données qui suivent en temps réel ces changements.* »

Pour limiter ces biais et mesurer l'impact des mesures de confinement sur la propagation du virus des entreprises privées (notamment des opérateurs de télécommunications) ont proposé d'utiliser leurs solutions d'analyse des flux de population à partir de l'usage des données de téléphonie mobile pour comprendre les déplacements de population et anticiper la circulation du virus.

Ces données agrégées en grande masse sont censées être anonymes et traitées statistiquement. Après les opérateurs de télécommunications, ce sont les entreprises du logiciel qui collectent des données de géolocalisation *via* des applications mobiles qui ont également annoncé produire des données agrégées. Cette profusion d'initiatives révèle par ailleurs l'intensité de la collecte de ces données de localisation par une grande pluralité d'acteurs.

❖ Les risques et enjeux posés par l'exploitation des données de localisation

La CNIL attire l'attention sur les enjeux qu'une telle exploitation, y compris sous une forme agrégée, est susceptible de faire peser sur les droits et libertés des personnes[26] :

- Les risques liés à l'usage des données de localisation, qui peuvent révéler des détails intimes sur la vie des citoyens, allant parfois jusqu'à dévoiler des informations sensibles[27] : activités politiques, convictions religieuses (par exemple, via la fréquentation de lieux de culte), mouvements et réseaux sociaux des personnes, etc.
- un manque de transparence et un risque de détournement de finalités ;
- des risques de ré-identification importants comme l'a démontré l'actualité à de multiples reprises (combinaison des données à des fins de ré-identification, etc.)[28]

La CNIL, et le CEPD dans ses lignes directrices du 21 avril 2020[29], ont insisté sur la nécessité de fonder un tel partage de données, en priorité, sur des données anonymisées lorsque cela permet de remplir l'objectif. Par exemple, les données détenues par les opérateurs de télécommunications peuvent être utiles pour suivre, de manière agrégée et anonyme, les mouvements des personnes, prévoir la propagation du virus et anticiper les besoins de santé publique.

Dans ce contexte, il est à noter que les organisations ont été confrontées à des défis techniques et ont dû envisager de développer des outils spécifiques pour permettre ce partage de données fiable, représentatif et interopérable. Cela nécessite d'être très vigilant sur la manière dont les données peuvent être utilisées stratégiquement pour faire face aux crises sanitaires et économiques à plusieurs niveaux.

4. Les « cahiers de rappel », une initiative complémentaire au dispositif national de traçage des « cas contacts »

En raison de l'aggravation de la situation sanitaire, certains établissements (restaurants, cafétérias, établissements de restauration rapide), situés dans les zones d'alerte maximale[30], ont été soumis, début octobre 2020, au respect d'un protocole sanitaire renforcé qui leur impose de tenir un « cahier de rappel » de leurs clients.

Ce « cahier de rappel », qui conditionne l'accès des clients à l'établissement est destiné à collecter leurs coordonnées afin de les tenir à disposition des autorités de sanitaires en cas de contamination de l'un des clients. Ce dispositif a donc vocation à compléter le dispositif national de traçage des « cas contacts »[31] en permettant, notamment, aux autorités sanitaires compétentes d'identifier un plus grand nombre de personnes exposées au virus au sein de zones considérées « à risque ».

Cette nouvelle initiative a pu susciter des craintes s'agissant du respect par les établissements concernés, notamment des TPE-PME, de la confidentialité des données ainsi collectées au regard notamment du caractère particulièrement exceptionnel du traitement considéré qui échappe à la gestion quotidienne de ce type de services. Dès lors, afin d'accompagner ces structures dans le respect

[26] Pour rappel, une communication relative à l'utilisation des données de localisation dans un contexte de crise sanitaire a fait l'objet d'une présentation orale à la séance plénière du 2 avril 2020.
[27] Stuart A. Thompson et Charlie Warzel. Twelve Million Phones, One Dataset, Zero Privacy. The New York Times, 19 décembre 2019.
[28] Nastasha Lomas. Techcrunch, 24 juillet 2019.
[29] [29] Lignes directrices 4/2020 relatives à l'utilisation de données de localisation et d'outils de recherche de contacts dans le cadre de la pandémie de COVID-19 [en ligne]. CEPD, 21 avril 2020. https://edpb.europa.eu/our-work-tools/our-documents/linee-guida/guidelines-042020-use-location-data-and-contact-tracing_fr
[30] Suite à cette première annonce, le nombre de zones en alerte maximale s'est progressivement étendu ce qui a conduit à l'application d'une telle mesure sur une large partie du territoire national.
[31] Au travers des fichiers « SI-DEP » et « Contact Covid », auxquels s'ajoute l'application « TousAntiCovid ».

de leurs obligations et surtout, de s'assurer du respect des principes de protection des données, la CNIL a rapidement publié (en parallèle de la publication du protocole sanitaire) :

- Des recommandations[32] concernant la mise en œuvre d'un tel dispositif (quelles données collecter, comment informer les personnes, quelle durée de conservation, quelles mesures de sécurité, etc.) ;
- Des exemples de formulaire de recueil de données et mentions d'information conformes au RGPD[33] (pour les zones où le dispositif est obligatoire ainsi que pour celles où le dispositif peut-être mis en œuvre sous réserve du consentement du client).

B. Surveiller le respect des mesures sanitaires

Loin d'être orchestrés par un pouvoir central dans une politique globale et cohérente, les dispositifs de surveillance sont pluriels et s'entremêlent, de manière concurrentielle ou complémentaire, par des acteurs aux intérêts multiples, à l'échelle locale, nationale, européenne voire internationale. Face à toutes ces initiatives, il est nécessaire de s'interroger sur la légitimité de ces dispositifs de surveillance pour gérer l'épidémie de coronavirus ainsi que sur leur conformité aux règles relatives à la protection des données. Les réponses à ces questions sont indispensables pour mettre en évidence l'équilibre, propre à chaque société, entre les moyens de lutte contre le virus et le respect des libertés fondamentales.

1. Caméras dites « intelligentes » et caméras thermiques : une myriade de solutions technologiques au soutien des politiques sanitaires

La lutte contre l'épidémie de COVID-19 a conduit certains acteurs à envisager de déployer des caméras dites « intelligentes » destinées notamment à mesurer la température, à détecter la présence de masques ou encore à s'assurer du respect de la distanciation sociale.

Ces dispositifs de surveillance utilisés pour gérer l'épidémie de coronavirus reposent sur des infrastructures informationnelles largement préexistantes à la crise sanitaire : en pratique, il s'agit soit de l'ajout d'une couche logicielle à des systèmes de vidéoprotection préexistants, soit du déploiement de nouveaux systèmes vidéo dédiés. Dans les deux cas, les fournisseurs de ces solutions se reposent sur des technologies utilisées dans les secteurs de la santé publique, du marketing ou encore de la sécurité et adaptés, aujourd'hui, à des fins de gestion de la pandémie.

Elles sont envisagés sur la voie publique voire dans (ou aux abords) des commerces, des transports ou encore des lieux de travail et sont susceptibles d'avoir des conséquences importantes pour les droits et libertés des citoyens qu'il s'agisse de passants, de clients ou de salariés.

❖ Les enjeux pour les libertés individuelles

Si les objectifs généralement assignés à ces dispositifs, c'est-à-dire participer à la lutte contre la propagation du virus ou veiller à la salubrité publique, sont le plus souvent légitimes, leur déploiement implique une collecte et une analyse systématiques de données d'individus circulant dans l'espace public ou dans des lieux recevant du public. **Leur développement incontrôlé présente donc le risque de généraliser un sentiment de surveillance chez les citoyens, de créer un phénomène de banalisation de technologies intrusives, et d'engendrer une surveillance**

[32] COVID-19 et les cahiers de rappel : les recommandations de la CNIL. CNIL, 7 octobre 2020. https://www.cnil.fr/fr/covid-19-et-les-cahiers-de-rappel-les-recommandations-de-la-cnil

[33] « Cahier de rappel » : exemples de formulaire de recueil de données et mentions d'information RGPD. CNIL, 7 octobre 2020. https://www.cnil.fr/fr/cahier-de-rappel-exemples-de-formulaire-de-recueil-de-donnees-et-mentions-dinformation-rgpd

accrue, susceptible de porter atteinte au bon fonctionnement de notre société démocratique.

L'espace public est en effet un lieu où s'exercent de nombreuses libertés individuelles : droit à la vie privée et à la protection des données à caractère personnel, liberté d'aller et venir, d'expression et de réunion, droit de manifester, liberté de conscience et d'exercice des cultes, etc. La préservation de l'anonymat dans l'espace public est une dimension essentielle pour l'exercice de ces libertés et la captation de l'image des personnes dans ces espaces est incontestablement porteuse de risques pour les droits et libertés fondamentaux de celles-ci.

Le déploiement massif de ces dispositifs de captation de l'image des individus et de détection de certains de leurs attributs, comportements ou émotions pourraient conduire, chez les personnes concernées, à une modification – voulue ou subie – de leurs comportements.

Les dispositifs qui seraient légalement mis en œuvre dans cette période doivent être considérés comme exceptionnels et rester proportionnés aux objectifs particuliers de cette période.

❖ Des garanties spécifiques doivent être apportées

La mise en œuvre éventuelle de tels systèmes de surveillance doit respecter le cadre légal applicable (RGPD, loi « Informatique et Libertés », directive « Police-Justice ») et être assortie de garanties de nature à préserver les libertés individuelles et particulièrement le droit à la vie privée.

C'est notamment pour ces raisons que les dispositifs de vidéoprotection, comme d'autres dispositifs de captation d'images dans l'espace public, font l'objet d'un encadrement législatif spécifique dans le Code de la sécurité intérieure. La CNIL **rappelle que l'usage des caméras « intelligentes », en revanche, n'est aujourd'hui pas prévu par un texte spécifique.** Leur utilité et intérêt réels, en fonction de circonstances précises, n'ont pu en ce sens être évalués et débattus à un niveau plus général que les organisations décidant de leur mise en place.

La CNIL, dans une publication du 17 juin 2020[34], a insisté sur la nécessité d'apporter un encadrement textuel adéquat, qui est requis dès lors que :

- des données sensibles sont traitées (la température corporelle dans le cas des caméras thermiques) ;
- ou que le droit d'opposition ne peut pas s'appliquer de manière effective (comme c'est souvent le cas en pratique dans l'espace public) .

Ce cadre textuel – nécessaire mais insuffisant – s'ajouterait à toutes les garanties que doivent prévoir ces éventuels dispositifs de vidéo « intelligente » au regard du RGPD (démonstration de leur nécessité et proportionnalité, durée de conservation limitée, mesures de pseudonymisation ou d'anonymisation, absence de suivi individuel, absence de traitement biométrique, etc.).

En outre, la CNIL rappelle que le déploiement de caméras thermiques (cf. encadré ci- dessous), qui traitent des données de santé, doit faire l'objet d'une attention toute particulière.

En effet, en dehors des problématiques de licéité du traitement de données concernant la santé, la CNIL tient à rappeler que l'efficacité et l'opportunité de la prise de température sont contestées dans la mesure où elle n'est pas un symptôme systématique du COVID-19, ou peut témoigner d'une autre infection. Pour les autorités sanitaires interrogées par la CNIL (voir annexe 1), un tel dispositif présente un risque de ne pas repérer les personnes infectées puisque certaines sont asymptomatiques et que le dispositif peut, en outre, être contourné par la consommation de produits antipyrétiques

[34] Caméras dites « intelligentes » et caméras thermiques : les points de vigilance de la CNIL et les règles à respecter [en ligne]. CNIL, 17 juin 2020. https://www.cnil.fr/fr/cameras-dites-intelligentes-et-cameras-thermiques-les-points-de-vigilance-de-la-cnil-et-les-regles

(médicaments permettant de diminuer la température corporelle, sans pour autant traiter les causes de la fièvre). A cet égard, le Haut Conseil de la Santé Publique[35] recommande d'ailleurs de ne pas

Contrôle de la température : un traitement de données à caractère personnel

Dans une démarche de prévention des contaminations, de nombreux acteurs (notamment les sociétés de transports mais également certaines communes ou, de manière plus générale, certains employeurs) ont souhaité mettre en place un contrôle de la température des clients, visiteurs ou employés à l'entrée de leurs locaux.

Au regard de la pluralité des dispositifs mis en œuvre, la qualification de traitement de données à caractère personnel a fait l'objet d'intenses discussions. Les réflexions menées ont permis de distinguer deux situations :

- **la seule vérification de la température au moyen d'un thermomètre manuel** (tel que par exemple de type infrarouge sans contact) à l'entrée d'un site, **sans qu'aucune trace ne soit conservée, ni qu'aucune autre opération ne soit effectuée** (tels que des relevés de ces températures, ou des remontées d'informations internes ou externes, etc.), ne relève pas de la règlementation en matière de protection des données.
- **les opérations automatisées de captation de température ou au moyen d'outils tels que des caméras thermiques** sont en revanche couvertes par la règlementation en matière de protection des données et font l'objet d'un encadrement spécifique (notamment s'agissant du traitement de données relatives à la santé).

mettre en place un dépistage du COVID-19 par prise de température dans la population.

2. Le recours aux drones dans le cadre du contrôle du respect des mesures de confinement

Depuis le début du confinement, la police et la gendarmerie ont utilisé des drones pour surveiller la population et faire appliquer les règles du confinement : diffusion des consignes par haut-parleurs, surveillance par vidéo pour repérer les contrevenants, etc.

Par une ordonnance de référé rendue le 18 mai 2020[36], le Conseil d'État a enjoint à « *l'État de cesser, sans délai, de procéder aux mesures de surveillance par drone, du respect, à Paris, des règles de sécurité sanitaire applicables à la période de déconfinement* ». Le Conseil d'État a estimé que, du fait de la possibilité de zoomer et d'identifier des personnes physiques, les dispositifs utilisés par la préfecture de police de Paris étaient soumis aux règles protégeant les données personnelles. Il a jugé que ces drones étaient utilisés en dehors du cadre prévu par la loi « Informatique et Libertés » et portaient une atteinte « *grave et manifestement illégale au droit au respect de la vie privée* ».

Comme mentionné précédemment, la CNIL a effectué plusieurs contrôles auprès du ministère de l'Intérieur et auprès de communes (polices municipales) ayant utilisé des drones durant la période de confinement.

[35] Contrôle d'accès par prise de température dans le cadre de l'épidémie à Covid-19. Haut Conseil de la Santé Publique. https://www.hcsp.fr/explore.cgi/avisrapportsdomaine?clefr=810
[36] Conseil d'État, Juge des référés, 18/05/2020, 440442, Inédit au recueil Lebon. https://www.legifrance.gouv.fr/ceta/id/CETATEXT000041897158/

CONCLUSION – Le numérique et les données à caractère personnel au cœur du débat public

La question de l'articulation entre les libertés individuelles et collectives et l'usage des technologies pour gérer la pandémie a été centrale dans le débat public, témoignant d'une préoccupation toujours plus grande de la population vis-à-vis des technologies de surveillance.

Face à la multitude d'initiatives qui auront émergée, la CNIL a su mobiliser ses deux piliers :

- **L'accompagnement :** la CNIL a accompagné l'ensemble de ses usagers, privés comme publics, professionnels comme particuliers, en publiant avis, fiches pratiques et recommandations en réponse aux nombreuses interrogations que la crise sanitaire a fait naître en matière de protection des données personnelles et de respect de la vie privée.
- **La chaine répressive :** la CNIL a joué pleinement son rôle en instruisant en priorité les réclamations liées à la COVID-19 et en menant des investigations des dispositifs mis en œuvre en réaction à la crise sanitaire afin de s'assurer que, malgré les circonstances exceptionnelles, le respect des droits et libertés fondamentaux des personnes concernées serait assuré.