

Note. #58

Pour une véritable minimisation des données au sein des entités publiques^[1]

**Dix propositions pour faire du principe le premier
rempart cybersécuritaire**



RAPHAËL MAUREL

Professeur de droit international public à l'Université
Bourgogne Europe – CREDIMI
Membre de l'Institut universitaire de France
Directeur du département éthique du numérique de l'OEP

Octobre 2026

^[1] La présente note a été rédigée par Raphaël Maurel et n'engage que son auteur.



Sommaire

En bref

3

Introduction

4

**Un principe clair en droit, massivement
ignoré en pratique**

7

**La minimisation comme premier rempart
cybersécuritaire**

17

Rendre la minimisation effective

20

Dix propositions

22

En bref

Le principe de minimisation des données consacré par l'article 5§1, c) du règlement général sur la protection des données constitue, depuis mai 2018, l'une des pierres angulaires du droit européen de la protection des données personnelles. Il impose au responsable de traitement de limiter la collecte, la conservation et le traitement des données personnelles à ce qui est strictement nécessaire à la finalité poursuivie. Alors que ce principe est juridiquement contraignant et qu'il est passible d'amendes administratives pouvant atteindre vingt millions d'euros ou 4% du chiffre d'affaires annuel mondial, sa méconnaissance massive par les entités publiques françaises – qu'il s'agisse de collectivités territoriales, établissements publics de coopération intercommunale, universités, hôpitaux, caisses, opérateurs d'État – constitue aujourd'hui une anomalie démocratique et un risque cybersécuritaire majeur. La succession de fuites de données survenues particulièrement depuis 2024 démontre que chaque donnée inutilement collectée est une donnée inutilement exposée, et que la pratique administrative française persiste à collecter, numériser, conserver et archiver des informations dont la nécessité n'a pas été vérifiée. Les causes sont connues : culture administrative du justificatif pour tout, absence de nomenclature nationale opposable des pièces strictement nécessaires, confusion entre présentation visuelle et collecte dématérialisée, formation insuffisante des agents, moyens et sanctions trop peu nombreux. La présente note formule à cet égard dix propositions concrètes articulées autour de cinq axes : interdire la collecte et la numérisation de certaines pièces manifestement excessives et promouvoir la validation visuelle, instituer un régime d'amendes administratives automatiques en cas d'exigence contraire à la minimisation, rendre visible et sensibiliser citoyens comme agents, accélérer la mise en œuvre effective du principe « dites-le nous une fois » déjà consacré en droit français depuis 2018 mais toujours insuffisamment déployé, et donner les moyens à la CNIL et aux entités publiques concernées de respecter leurs obligations. Il s'agit à la fois de protéger les droits fondamentaux des usagers, d'économiser les deniers publics mobilisés par la gestion et la protection de données inutiles, et de renforcer la cybersécurité collective en réduisant à la source la surface d'attaque qu'offrent aujourd'hui les entités publiques françaises aux acteurs malveillants.

Introduction

Les deux dernières années ont vu la France connaître une série de fuites de données personnelles sans précédent par leur ampleur et leur fréquence. En février 2024, les opérateurs de tiers payant Viamedis et Almerys exposaient les données de plus de trente-trois millions de personnes assurées^[2]. Un mois plus tard, en mars 2024, France Travail et Cap emploi annonçaient à la Commission nationale de l'informatique et des libertés que les données de potentiellement quarante-trois millions de personnes avaient été extraites de leurs systèmes d'information^[3] – soit, en valeur absolue, la plus importante fuite de l'histoire du pays. L'année 2025 a vu se multiplier les incidents visant les universités françaises, de l'Université de Lille, dont deux mille étudiants ont été exposés fin décembre^[4], à Grenoble École de Management^[5], en passant par Paris 1 Panthéon-Sorbonne^[6]. L'année 2026 a été marquée, notamment, par les attaques en cascade dirigées contre le ministère de l'Éducation nationale, affectant successivement les systèmes Compas, ÉduConnect et SI Formation, et culminant à l'été avec la circulation sur des forums spécialisés de plusieurs centaines de millions de lignes de données brutes couvrant la totalité des académies^[7].

La réponse publique à cette série d'incidents s'est jusqu'ici concentrée sur deux leviers, si l'on excepte le volet pénal qui concerne la (difficile) poursuite des responsables : le renforcement des mesures techniques de cybersécurité (sauvegardes, chiffrement, détection d'intrusion, authentification multi-facteurs) et la montée en puissance de l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Ces deux leviers sont essentiels, mais à l'évidence insuffisants.

^[2] Les données concernées incluent identité, numéro de sécurité sociale, nom de la complémentaire santé, période et nature des droits de personnes assurées.

^[3] Communiqué de France Travail et de Cap emploi du 13 mars 2024 et communiqué CNIL du même jour : intrusion dans les systèmes d'information entre le 6 février et le 5 mars 2024, extraction potentielle des données de 43 millions de personnes couvrant les demandeurs d'emploi actuels et ceux inscrits dans les vingt dernières années ; données concernées : noms, prénoms, dates de naissance, numéros de sécurité sociale, identifiants France Travail, adresses postales et électroniques, numéros de téléphone.

^[4] Cyberattaque révélée le 29 décembre 2025 par le groupe « Scattered LAPSUS\$ Hunters » visant l'Université de Lille (plus de 80 000 étudiants) ; échantillon publié portant sur environ 2 000 étudiants, incluant données administratives et dates de naissance.

^[5] Cyberattaque révélée le 29 décembre 2025 à l'encontre de Grenoble École de Management ; données affectées correspondant à une liste de diffusion issue d'un système de gestion de la relation client.

^[6] Fuite de données publiée en 2025 à l'Université Paris 1 Panthéon-Sorbonne : extraction de données « non confidentielles » issues de l'annuaire public à partir d'un compte utilisateur usurpé.

^[7] Communiqué intersyndical FNEC-FP-FO du 23 août 2026 : succession d'incidents visant les systèmes d'information de l'Éducation nationale au premier semestre 2026 (Compas en mars, ÉduConnect en avril, SI Formation en juillet, puis fuite d'environ 346 millions de lignes de données brutes couvrant 33 académies à la mi-août).

La question que l'on veut poser ici est celle de savoir pourquoi France Travail conservait, à la date de la fuite, les données de personnes inscrites sur ses listes jusqu'à vingt ans auparavant^[8]. De manière similaire, on peut questionner la raison pour laquelle les communes exigent chaque année la fourniture d'une copie des pages de vaccination du carnet de santé des enfants alors qu'aucune règle n'impose autre chose qu'une vérification visuelle^[9] ; la raison pour laquelle une université demande automatiquement un relevé d'identité bancaire à un conférencier invité pour une intervention sans aucun flux financier ; ou encore la raison pour laquelle les systèmes d'information scolaires conservent plus de sept millions de bulletins scolaires accessibles depuis un seul compte compromis.

Chacune de ces données inutilement collectées est devenue, comme ces affaires récentes le démontrent, une donnée inutilement exposée. Le principe de minimisation, consacré depuis mai 2018 par l'article 5§1, point c) du règlement général sur la protection des données^[10], et dont l'absence de respect est passible d'amendes administratives pouvant atteindre vingt millions d'euros ou 4% du chiffre d'affaires annuel mondial (pour une entreprise)^[11], n'est pourtant pas une obligation juridique abstraite. Au-delà de son existence incontestable – bien que manifestement méconnue – en droit des données, il s'agit aussi, et peut-être avant tout, d'une mesure de cybersécurité évidente, dont la mise en œuvre défailante constitue aujourd'hui l'une des principales vulnérabilités systémiques des entités publiques françaises.

La présente note, qui prend acte du fait que la cybersécurité est d'abord une question d'éthique et implique donc la création d'une culture du questionnement à propos du sens de nos pratiques, s'efforce de rappeler cette articulation fondamentale entre

^[8] France Travail invoque, pour justifier la conservation des données vingt ans après la dernière cessation d'inscription, l'alinéa 1 de l'article R. 5312-44 du code du travail. Dans sa version issue de la rédaction du Décret n° 2024-1268 du 31 décembre 2024 (relatif au système d'information de l'opérateur France Travail et portant diverses dispositions relatives aux traitements de données à caractère personnel dans le champ de l'emploi, de l'insertion et de la formation professionnelle), celui-ci dispose que « [...]es données à caractère personnel et les informations enregistrées dans le traitement automatisé mentionné à l'article R. 5312-38 sont conservées, dans la mesure où les finalités du traitement l'exigent, en base active pendant une durée maximale de dix ans à compter de la cessation d'inscription sur la liste des demandeurs d'emploi, sans dépasser une durée totale de vingt ans et sans préjudice des durées de conservation fixées dans les traitements comportant une durée inférieure ». On peut sérieusement questionner la mesure dans laquelle les « finalités du traitement » exigent une telle durée de conservation.

^[9] V. par ex. Agence régionale de santé Hauts-de-France, « Élus : enfants en collectivité et contrôle des vaccinations obligatoires, quel rôle du maire ? », qui rappelle que les maires et directeurs d'école doivent se faire présenter le carnet de santé ou un document attestant la réalisation des vaccinations, sans que la conservation d'une copie ne soit juridiquement requise.

^[10] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (RGPD), article 5, paragraphe 1, point c) : les données à caractère personnel doivent être « adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données) ».

^[11] Règlement (UE) 2016/679, article 83, paragraphe 5, point a) : les violations du principe de minimisation font partie des violations les plus graves, passibles d'amendes administratives s'élevant jusqu'à 20 000 000 d'euros ou 4 % du chiffre d'affaires annuel mondial.

minimisation et cybersécurité, afin d'en tirer des propositions concrètes.

Elle expose d'abord le cadre juridique du principe de minimisation et dresse le constat de l'écart (considérable) entre le droit et la pratique dans le secteur public, en s'appuyant sur des exemples ordinaires qui, mis bout à bout, dessinent une véritable pathologie administrative. Elle démontre ensuite pourquoi la minimisation doit être pensée comme un instrument de sécurité des systèmes d'information, et pas seulement comme une obligation de conformité au règlement européen, en s'appuyant sur les modèles comparés – au premier rang desquels le modèle estonien, qui a fait du principe du « once-only » la pierre angulaire de son administration numérique. Elle formule enfin dix propositions opérationnelles articulées autour de cinq axes, lesquelles sont destinées à rendre la minimisation effective dans les entités publiques françaises.

Un principe clair en droit, massivement ignoré en pratique

Le principe de minimisation des données constitue l'un des piliers du droit européen de la protection des données personnelles. Sa valeur normative est incontestable et incontestée ; son champ d'application est universel. Son application effective par les entités publiques françaises est, en revanche, particulièrement défailante.

Un socle juridique incontestable

L'article 5 du règlement général sur la protection des données du 27 avril 2016 est ainsi rédigé :

Article 5 - Principes relatifs au traitement des données à caractère personnel

1. Les données à caractère personnel doivent être :

a) traitées de manière licite, loyale et transparente au regard de la personne concernée (licéité, loyauté, transparence);

b) collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités; le traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques n'est pas considéré, conformément à l'article 89, paragraphe 1, comme incompatible avec les finalités initiales (limitation des finalités);

c) adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données);

d) exactes et, si nécessaire, tenues à jour; toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder (exactitude);

e) 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; les données à caractère personnel peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1, pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées requises par le présent règlement afin de garantir le

es droits et libertés de la personne concernée (limitation de la conservation);

f) traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité);

2. Le responsable du traitement est responsable du respect du paragraphe 1 et est en mesure de démontrer que celui-ci est respecté (responsabilité).

L'article 5§1, c) impose donc au responsable de traitement de limiter la collecte des données personnelles à ce qui est « adéquat, pertinent et nécessaire » au regard des finalités poursuivies.

Ce principe est repris, en droit interne, par la loi du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés^[12]. Il est complété par l'obligation plus générale de sécurité du traitement codifiée à l'article 32 du règlement, qui requiert, « [c]ompte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques », la mise en œuvre de mesures techniques et organisationnelles appropriées au risque^[13].

Sa méconnaissance est passible, en vertu de l'article 83§5 du même règlement, d'amendes administratives pouvant s'élever jusqu'à vingt millions d'euros ou, pour les entreprises, 4% du chiffre d'affaires annuel mondial, le montant le plus élevé étant retenu :

*Article 83 - Conditions générales pour imposer des amendes administratives
[...]*

5. Les violations des dispositions suivantes font l'objet, conformément au paragraphe 2, d'amendes administratives pouvant s'élever jusqu'à 20 000 000 EUR ou, dans le cas d'une entreprise, jusqu'à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu :

a) les principes de base d'un traitement, y compris les conditions applicables au consentement en vertu des articles 5, 6, 7 et 9 ;

b) les droits dont bénéficient les personnes concernées en vertu des articles 12 à 22 ;

c) les transferts de données à caractère personnel à un destinataire situé dans un pays tiers ou à une organisation internationale en vertu des articles 44 à 49 ;

^[12] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, telle que modifiée par la loi n° 2018-493 du 20 juin 2018 et l'ordonnance n° 2018-1125 du 12 décembre 2018.

^[13] Règlement (UE) 2016/679, article 32, « sécurité du traitement ».

d) toutes les obligations découlant du droit des États membres adoptées en vertu du chapitre IX ;

e) le non-respect d'une injonction, d'une limitation temporaire ou définitive du traitement ou de la suspension des flux de données ordonnée par l'autorité de contrôle en vertu de l'article 58, paragraphe 2, ou le fait de ne pas accorder l'accès prévu, en violation de l'article 58, paragraphe 1.

Le Comité européen de la protection des données a de son côté adopté en octobre 2020 ses lignes directrices sur la protection des données dès la conception et par défaut, qui font de la minimisation l'une des huit obligations centrales de l'article 25 du RGPD^[14]. Le délégué à la protection des données institué par les articles 37 à 39 du RGPD constitue logiquement, dans chaque entité publique, l'interlocuteur légal naturel pour la mise en œuvre du principe de minimisation.

La Commission nationale de l'informatique et des libertés a, en France, largement fait sienne ces dispositions claires, et publié de longue date une fiche thématique claire précisant la portée du principe^[15]. La méthode d'analyse d'impact relative à la protection des données diffusée par la CNIL requiert, par ailleurs et à titre de première étape, l'évaluation du caractère nécessaire et proportionné du traitement^[16]. Enfin, la CNIL inscrit chaque année la minimisation parmi ses priorités thématiques de contrôle, avec une attention particulière, depuis 2024, aux dispositifs ciblant les mineurs^[17].

^[14] Comité européen de la protection des données, lignes directrices 4/2019 relatives à la protection des données dès la conception et par défaut, adoptées le 20 octobre 2020. L'article 25§1 du RGPD se lit par ailleurs ainsi : « Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, que présente le traitement pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation, qui sont destinées à mettre en œuvre les principes relatifs à la protection des données, par exemple la minimisation des données, de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du présent règlement et de protéger les droits de la personne concernée » (nous soulignons).

^[15] Commission nationale de l'informatique et des libertés, fiche thématique « Les principes applicables au traitement de données personnelles – Le principe de minimisation », cnil.fr/fr/les-principes-cles-du-rgpd.

^[16] Commission nationale de l'informatique et des libertés, méthode d'analyse d'impact relative à la protection des données (AIPD, 2018, mise à jour 2023), prévoyant l'évaluation du caractère nécessaire et proportionné du traitement, en premier lieu au regard du principe de minimisation.

^[17] Commission nationale de l'informatique et des libertés, programme de contrôles 2024 : vérification du respect du principe de minimisation par les sites et plateformes ciblant les enfants et adolescents, en complément des recommandations relatives aux droits des mineurs dans l'environnement numérique.

Le droit français est à vrai dire allé plus loin encore que ce que le règlement européen prescrit en instituant, par la loi du 10 août 2018 pour un État au service d'une société de confiance, dite loi ESSOC, le principe du « dites-le nous une fois »^[18] et son corollaire qu'est le droit, pour l'usager (ou à tout le moins certains d'entre eux), de ne pas produire des informations ou données qu'une administration détient déjà ou peut obtenir d'une autre administration participant au système d'échange. Placé en tête d'un titre II intitulé « Vers une action publique modernisée, simple et efficace », l'article 40 de la loi ESSOC dispose ainsi que :

« Sans préjudice de l'article L. 114-8 du code des relations entre le public et l'administration, à titre expérimental et pour une durée de trois ans à compter de la publication du décret en Conseil d'État prévu au troisième alinéa du présent article, les personnes inscrites au répertoire des entreprises et de leurs établissements, qui y consentent, ne sont pas tenues de communiquer à une administration des informations que celle-ci détient déjà dans un traitement automatisé ou qui peuvent être obtenues d'une autre administration par un tel traitement.

Lorsqu'elle obtient des informations par un traitement automatisé, l'administration en informe la personne concernée. Elle assure la confidentialité et la protection de ces informations afin d'empêcher qu'elles soient déformées ou endommagées ou que des tiers non autorisés y aient accès.

Un décret en Conseil d'État, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés, précise les modalités d'application du présent article, notamment la liste des traitements automatisés entrant dans le champ de l'expérimentation ainsi que, pour chaque traitement, la liste des données disponibles.

L'expérimentation fait l'objet d'une évaluation, notamment de son impact sur les délais administratifs, dont les résultats sont transmis au Parlement ».

Ce droit a été renforcé par la loi du 21 février 2022 relative à la différenciation, la décentralisation, la déconcentration et portant diverses mesures de simplification de l'action publique locale, dite loi 3DS, qui a introduit un nouvel article L. 113-12 au code des relations entre le public et l'administration^[19], en complément des articles L. 114-8 et L. 114-9 préexistants^[20], et par le décret d'application du 11 mai 2023^[21].

^[18] Loi n° 2018-727 du 10 août 2018 pour un État au service d'une société de confiance.

^[19] Code des relations entre le public et l'administration, article L. 113-12 créé par la loi n° 2022-217 du 21 février 2022 : « [u]ne personne présentant une demande ou produisant une déclaration à une administration ne peut être tenue de produire des informations ou des données que celle-ci détient ou qu'elle peut obtenir directement auprès d'une administration participant au système d'échange de données ».

^[20] V. le Code des relations entre le public et l'administration, articles L. 114-8 et L. 114-9, dans leur rédaction issue de la loi n° 2016-1321 du 7 octobre 2016 et de la loi n° 2018-727 du 10 août 2018 pour un État au service d'une société de confiance (ESSOC).

^[21] Décret n° 2023-361 du 11 mai 2023 relatif aux échanges d'informations et de données entre administrations dans le cadre de démarches administratives, pris en application de la loi 3DS, JORF du 12 mai 2023.

Poussant plus loin le principe déjà ancien selon lequel « les autorités administratives échangent entre elles toutes informations ou données strictement nécessaires pour traiter les demandes présentées par un usager ou les déclarations transmises par celui-ci en application d'un texte législatif ou réglementaire » (article 16 A de la Loi n° 2000-321 du 12 avril 2000 relative aux droits des citoyens dans leurs relations avec les administrations, avant son abrogation par l'ordonnance n°2015-1341 du 23 octobre 2015), l'article L.113-12 du CRPA prévoit ainsi que « [u]ne personne présentant une demande ou produisant une déclaration à une administration ne peut être tenue de produire des informations ou des données que celle-ci détient ou qu'elle peut obtenir directement auprès d'une administration participant au système d'échange de données défini à l'article L. 114-8 » – lequel vise toutes les administrations. La seule limite à ce système d'échange est la mesure de transparence prévue au III de cet article 114-8, selon lequel « [l]a liste des administrations qui se procurent directement des informations ou des données auprès d'autres administrations françaises en application du présent article, la liste des informations ou des données ainsi échangées et le fondement juridique sur lequel repose le traitement des procédures mentionnées au I du présent article font l'objet d'une diffusion publique dans les conditions prévues à l'article L. 312-1-1 ».

Le principe « dites-le nous une seule fois », en tant que dérivé du principe de minimisation, est ainsi, en droit français, à la fois un droit subjectif de l'usager et une contrainte procédurale opposable à l'administration. En droit européen, le règlement sur le portail numérique unique du 2 octobre 2018 a également consacré le principe « une seule fois » pour les démarches transfrontalières à compter du 12 décembre 2023. L'article 14 du Règlement institue en effet un « système technique pour l'échange automatisé de justificatifs entre autorités compétentes de différents États membres » (§1), « n'est pas obligatoire pour les utilisateurs et n'est autorisée qu'à leur demande expresse, sauf disposition contraire du droit de l'Union ou du droit national » (§4) mais permet d'éviter les redondances de données : « [l]orsqu'un utilisateur concerné leur en fait expressément la demande, de manière libre, spécifique, éclairée et univoque, les autorités compétentes responsables des procédures en ligne visées au paragraphe 1 sollicitent le justificatif directement auprès des autorités de délivrance du justificatif compétentes dans les autres États membres par l'intermédiaire du système technique»^[22].

Au-delà de la consécration du principe « dites-le nous une fois » puis de son renforcement par la loi 3DS du 21 février 2022, la Direction interministérielle du numérique (Dinum) a créé en décembre 2019 un guichet dédié à l'accompagnement des acteurs publics, et chiffrait la même année à 320 millions d'euros par an les économies potentielles d'une généralisation effective^[23].

^[22] Règlement (UE) 2018/1724 du Parlement européen et du Conseil du 2 octobre 2018 établissant un portail numérique unique (Single Digital Gateway), article 14§7.

^[23] La Gazette des communes, 2 juillet 2019 (<https://www.lagazettedescommunes.com/629133/ou-en-est-la-parution-des-decrets-relatifs-au-programme-dites-le-nous-une-fois/>).

Le dispositif FranceConnect permet depuis plusieurs années la justification de l'identité et le pré-remplissage automatique des données fiscales et sociales dans les démarches en ligne^[24]. L'API Entreprise et l'API Particulier offrent aux administrations et aux organismes de service public des interfaces techniques permettant d'obtenir directement les données déjà détenues ailleurs^[25].

L'obstacle à la mise en œuvre du principe de minimisation n'est donc pas l'absence d'instruments ou de règles, mais l'absence de contrainte à leur usage effectif.

Une pratique administrative qui ignore massivement le principe

Face à cet appareil juridique dense, cohérent et limpide, la pratique administrative française se caractérise, de manière frappante, par son indifférence totale.

Les exemples qui suivent, loin d'être exceptionnels, décrivent le fonctionnement ordinaire des guichets publics. Dans la mesure où il ne saurait s'agir ici de dénoncer, mais plutôt d'identifier des difficultés, aucune citation directe et nominative ne s'impose.

Une commune exige chaque année, lors de l'inscription aux accueils périscolaires, la fourniture d'une copie des pages de vaccination du carnet de santé de chaque enfant, à laquelle s'ajoutent parfois une copie de l'attestation versée par la caisse d'allocations familiales, un certificat médical et une ou deux photographies – alors que la réglementation sanitaire n'impose au maire ou au directeur d'école qu'une vérification visuelle du carnet. Une école municipale d'art requiert, alors même qu'elle répond de la même administration que les services périscolaires, exactement les mêmes documents.

Certains établissements d'enseignement supérieur demandent encore systématiquement un relevé d'identité bancaire à tout intervenant extérieur, y compris lorsque l'intervention n'est associée à aucun flux financier – dans le cas contraire, la transmission d'un RIB paraît évidemment indispensable, dès lors que le chèque bancaire est en voie de disparition. Tel est le cas très répandu de la conférence ou de l'intervention en colloque donnée à titre gratuit ou encore de la participation à un jury de thèse, le déplacement et l'hébergement de la personne étant alors directement pris en charge par l'institution accueillante. L'exigence de communiquer le numéro de Sécurité sociale et la date de naissance de la personne intervenante ne s'explique pas davantage dans ces situations, à l'exception des rares cas où ces informations sont requises, à des fins d'identification, par un service de sécurité à l'entrée de l'établissement.

^[24] FranceConnect est un dispositif d'identification électronique de l'État opéré par la Direction interministérielle du numérique.

^[25] API Entreprise et API Particulier, deux interfaces de programmation de l'État permettant aux administrations et à certains organismes privés chargés d'une mission de service public d'accéder, dans le cadre fixé par le CRPA, aux données déjà détenues par d'autres administrations.

La durée de conservation de ces données, allant généralement de trois à cinq ans, n'est par ailleurs justifiée par aucune finalité sérieuse.

Des mairies exigent encore, lors d'une démarche d'état civil, la production de justificatifs multiples que l'administration pourrait obtenir directement par le dispositif « dites-le nous une fois » si celui-ci était effectivement activé. Des établissements publics hospitaliers conservent des documents numérisés dont la finalité première est éteinte depuis plusieurs années, sans avoir engagé aucune procédure de suppression.

Les causes de cette défaillance sont aisément identifiables. On peut en relever au moins six.

Elles résident, en tout premier lieu, dans une culture administrative du justificatif pour tout, héritée d'un rapport historiquement défiant à l'usager (l'institution collecte et conserve la donnée « au-cas-où » elle serve un jour, l'usager étant parfois jugé incapable ou susceptible de devenir incapable de la produire ultérieurement).

Une deuxième explication est l'absence d'une nomenclature nationale opposable des pièces strictement nécessaires par type de démarche. Il en découle que chaque entité publique détermine, à son niveau et souvent sans réflexion spécifique à ce sujet, la liste des documents exigés sans contrôle extérieur systématique.

En troisième lieu, il faut admettre qu'il existe une confusion persistante entre la présentation visuelle d'une pièce et sa collecte dématérialisée. Les agents, formés à exiger la pièce, sont rarement formés à la restituer après vérification. Ainsi, un memo ou une procédure interne prescrira par défaut volontiers une photocopie ou un scan de toute pièce produite pour insertion dans un dossier, alors qu'une simple vérification visuelle suffit. Cette habitude résulte parfois d'une recherche de déresponsabilisation des agents, dont la qualité ou l'existence de la vérification visuelle opérée pourrait être contestée : dans le doute et afin d'éviter toute mise en difficulté ultérieure de l'agent, la pièce de l'usager est collectée et conservée.

En quatrième lieu, l'observation du terrain démontre une formation gravement insuffisante des agents publics au principe de minimisation, qui n'est pas intégré de manière systématique dans les cursus ni de l'Institut national du service public (bien qu'il faille espérer que ses étudiant(e)s y soient sensibilisés), ni des instituts régionaux d'administration, ni du Centre national de la fonction publique territoriale, ni des écoles de la fonction publique. De manière plus générale, alors même que le RGPD a été adopté il y a plus de dix ans, sa diffusion au sein même de l'administration reste aujourd'hui, par réticence et par manque de moyens de formation des agents, très lacunaire. Ni les élu(e)s – à l'exception de celles et ceux qui exercent une profession dans le secteur privé qui est davantage sensibilisé à la protection des données – ni les agents ne sont ainsi réellement formés à cet enjeu considéré, face aux urgences permanentes et aux enjeux budgétaires auxquelles font face les collectivités territoriales, comme secondaire.

En cinquième lieu, cette défaillance structurelle peut être reliée au très faible nombre de sanctions prononcées par la Commission nationale de l'informatique et des libertés à l'encontre des entités publiques.

Le bilan 2024 fait en effet état de 87 sanctions, 180 mises en demeure et 64 rappels à la loi, dont la part publique reste minoritaire malgré une accentuation récente^[26]. La première sanction pécuniaire d'une commune n'a été prononcée qu'en 2023, après un parcours administratif globalement long^[27]. Dit autrement, le dispositif de sanction n'est pas dissuasif, ce qui est partiellement lié aux moyens limités de la CNIL et à la volonté, assez largement partagée, de limiter les sanctions prononcées contre des collectivités territoriales déjà en difficulté budgétaire – la charge des amendes reposant nécessairement, *in fine*, sur le contribuable-usager, ce qui paraît paradoxal.

Cette défaillance peut enfin tenir au défaut, au bénéfice des usagers, d'outils simples permettant de signaler en temps réel à la CNIL un manquement constaté au guichet.

On pourrait ajouter à cette liste déjà dense d'autres conclusions, à commencer par un décalage entre les mesures correctrices adoptées par l'État et les moyens mis en œuvre pour les faire appliquer concrètement. Ainsi, les décrets d'application du principe « dites-le-nous une fois » prévoient le partage d'une liste limitée de pièces justificatives, qui s'est étoffée progressivement mais reste très en-deçà du spectre réel des démarches administratives ; l'adoption de FranceConnect par les administrations locales reste inégale ; l'API Entreprise et l'API Particulier sont peu connues et peu mobilisées hors des champs fiscal et social. Enfin, l'absence de réflexion sur le statut du délégué à la protection des données conduit notamment à ce que ceux-ci soient peu mobilisés au sein des entités publiques ; ou qu'à l'inverse qu'ils soient, du fait de leur mutualisation sur un trop grand nombre de collectivités, placés dans l'incapacité de remplir leur office de sensibilisation et de conseil^[28].

Des conséquences dramatiques

Ces pratiques administratives connues, fondées souvent sur une méconnaissance du droit applicable et à l'évidence illégales pourraient, d'un point de vue autre que juridique, ne pas être considérées comme particulièrement problématiques...si elles ne conduisaient pas à des fuites de données majeures dont l'accélération est effrayante.

L'hypothèse selon laquelle une donnée inutilement collectée est une donnée inutilement exposée trouve en effet, dans la succession des fuites de données survenues depuis 2024, une illustration systémique. Comme on l'a signalé en introduction, France Travail a annoncé le 13 mars 2024 avoir été victime, entre le 6 février et le 5 mars, d'une intrusion ayant conduit à l'extraction potentielle des données de 43 millions de personnes couvrant les demandeurs d'emploi actuels et ceux inscrits

^[26] Commission nationale de l'informatique et des libertés, « Sanctions et mesures correctrices : bilan 2024 de l'action de la CNIL », communiqué du 5 février 2025 faisant état de 87 sanctions, 180 mises en demeure et 64 rappels à la loi prononcés en 2024, pour un montant cumulé des amendes atteignant 55 millions d'euros. Le communiqué et le bilan montrent une forte augmentation des mesures correctrices portée par la procédure simplifiée.

^[27] Commission nationale de l'informatique et des libertés, bilan 2023 (publié le 16 février 2024). La première sanction pécuniaire d'une commune française confirme d'ailleurs l'applicabilité du régime répressif aux collectivités territoriales ayant persisté dans leurs manquements après mise en demeure.

^[28] V. sur ce sujet R. Maurel, « Pour un régime juridique du délégué à la protection des données », Note n°56 de l'Observatoire de l'éthique publique, septembre 2026.

dans les vingt dernières années.

L'incident fait suite, pour le même opérateur, à l'affaire Majorel de l'été 2023, qui avait déjà exposé les données de dix millions de personnes^[29].

Les attaques dirigées contre les prestataires de tiers payant Viamedis et Almerys, en février 2024, ont exposé les données de plus de 33 millions de personnes assurées, incluant leur numéro de sécurité sociale, la nature de leur couverture complémentaire et la période de couverture – soit un « gisement » considérable de données, permettant des combinaisons avec d'autres bases à des fins d'usurpation d'identité. L'Éducation nationale a cumulé en 2026 une série d'incidents dont l'ampleur dépasse celle, pourtant déjà historique, de France Travail : exploitation de la faille ÉduConnect pouvant concerner 3,5 millions d'élèves, circulation de 7,2 millions de bulletins scolaires sur des forums spécialisés^[30], puis fuite estimée à 346 millions de lignes de données brutes couvrant les 33 académies, affectant successivement les systèmes Compas en mars, ÉduConnect en avril et SI Formation en juillet. Les universités françaises n'ont pas été épargnées ; on dénombre une fuite de données concernant 117 000 personnes à Toulouse en février 2020^[31], une extraction de données d'annuaire à Paris 1 en 2025, une intrusion informatique à l'Université de Lille revendiquée fin décembre 2025 par le groupe Scattered LAPSUS\$ Hunters, une cyberattaque contre Grenoble École de Management le même mois, ou encore une revendication contre Nantes Université le 28 juillet 2026^[32]. L'Agence nationale de la sécurité des systèmes d'information documente plus généralement, dans ses panoramas annuels de la cybermenace 2024 et 2025, une augmentation structurelle des attaques visant le secteur public, et au premier chef l'enseignement supérieur et la recherche^[33].

La lecture de cette série très lacunaire, tant les fuites de données sont quotidiennes, fait apparaître une régularité : dans chacune de ces affaires, la question de la nécessité de la collecte et de la durée de conservation n'a été posée qu'après l'incident, et par les commentateurs plutôt que par les responsables de traitement eux-mêmes. Rien n'obligeait en effet France Travail à conserver pendant vingt ans les coordonnées de personnes sans lien actif avec le service ; rien n'obligeait l'Éducation nationale à centraliser dans un même système accessible depuis le réseau Internet 7,2 millions de bulletins scolaires concernant plusieurs années de scolarité ; rien n'obligeait les universités à agréger dans des bases d'administration la totalité des coordonnées de leurs anciens étudiants et anciens personnels.

^[29] Incident de l'été 2023 : vol de données chez Majorel, prestataire de Pôle emploi, portant sur dix millions de personnes (nom, prénom, statut actuel ou ancien de demandeur d'emploi, numéro de sécurité sociale).

^[30] Ministère de l'Éducation nationale, communiqué du 14 avril 2026. L'exploitation, fin 2025, d'une faille d'ÉduConnect par usurpation d'identité fait, selon les éléments relayés publiquement, que 3,5 millions d'élèves pourraient être concernés ; une base complémentaire d'environ 7,2 millions de bulletins scolaires serait en circulation sur des *fora* spécialisés.

^[31] Fuite de février 2020 des données informatiques de 105 000 étudiants et 12 000 personnels de l'Université fédérale Toulouse Midi-Pyrénées, consécutive à une opération de vote électronique par un prestataire tiers.

^[32] Revendication publiée le 28 juillet 2026 par un acteur malveillant visant deux sous-domaines de Nantes Université, portant sur 1 835 comptes utilisateurs annoncés comme compromis.

^[33] Agence nationale de la sécurité des systèmes d'information, Panorama annuel de la cybermenace 2024 et 2025.

Il semble donc bien que l'absence de politique de minimisation effective explique, bien souvent, l'ampleur disproportionnée des fuites. Par-delà cette lacune, il faut aussi interroger l'absence de réflexion éthique qui caractérise l'action de collecte systématique de données inutiles.

La minimisation comme premier rempart cybersécuritaire

Dans ce contexte dramatique et en constante aggravation, le principe minimisation des données ne peut plus être conçu et compris comme une contrainte de conformité étrangère ou périphérique à la cybersécurité. Il est une mesure de cybersécurité en tant que telle, et plus encore, probablement la plus efficace par rapport à son coût. Toutes les autres mesures techniques et organisationnelles – chiffrement, authentification multi-facteurs, détection d'intrusion, segmentation réseau, sauvegardes, plans de continuité – protègent en effet des données contre un attaquant. Pour sa part, la minimisation réduit, en amont, la quantité de données exposées à cet attaquant. Elle agit donc sur la surface d'attaque, et non sur la hauteur du bouclier dressé pour s'en défendre.

L'absence de collecte, meilleure mesure de cybersécurité

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) rappelle, dans son Guide d'hygiène informatique régulièrement mis à jour, une évidence : la réduction du volume de données traitées constitue une mesure de sécurité de premier rang^[34], parce qu'elle réduit mécaniquement l'exposition en cas de compromission.

Cette évidence technique avait déjà été réaffirmée par l'article 32 du règlement général sur la protection des données, qui lie étroitement sécurité du traitement et principes de l'article 5 (dont la minimisation). Encore faut-il préciser que le lien entre minimisation et sécurité ne se limite pas à la seule quantité de données affectées en cas d'incident. La sobriété du traitement – c'est-à-dire la minimisation – diminue également les combinaisons possibles entre jeux de données. Concrètement, un attaquant qui dispose du numéro de sécurité sociale, de l'identité et de la date de naissance d'une personne peut, par croisement avec une autre base, reconstituer un profil, ce qui ouvre la voie vers une usurpation d'identité. Un attaquant qui ne dispose que de l'identité et de la date de naissance ne le peut généralement pas. Autrement dit, chaque donnée collectée au-delà du strict nécessaire élève la valeur économique de la base de données capturée par les acteurs malveillants, et par ricochet la probabilité d'une attaque ciblée.

Cette articulation est particulièrement importante pour les entités publiques, dont les traitements concentrent souvent des données par nature sensibles et difficilement

^[34] Agence nationale de la sécurité des systèmes d'information, Guide d'hygiène informatique (2017), en ligne (<https://messervices.cyber.gouv.fr/guides/guide-dhygiene-informatique>).

remplaçables : numéro de sécurité sociale pour les caisses, données scolaires sur plusieurs années pour l'Éducation nationale, parcours professionnel sur plusieurs décennies pour France Travail, données médicales pour les hôpitaux, les écoles et les crèches, données familiales pour les communes et autres collectivités. Chacune de ces bases agrège plusieurs catégories de données personnelles, ce qui lui fait atteindre rapidement une valeur marchande importante sur les marchés clandestins. La politique de minimisation est donc, pour une entité publique, un investissement cybersécuritaire d'un rendement supérieur à toute autre mesure défensive, et dont le coût de mise en œuvre est, à long terme, inférieur à celui des mesures techniques équivalentes (pour peu qu'elles existent). La minimisation épargne évidemment, en effet, les coûts de stockage, de maintenance, de sauvegarde, de chiffrement et de notification en cas d'incident.

L'exemple estonien

L'Estonie offre, depuis 2001, un modèle d'administration numérique intéressant, construit à partir du principe du « *once-only* ». Son architecture repose sur X-Road, infrastructure d'échange de données entre bases distribuées, qui ne centralise aucune donnée mais permet aux registres publics – registre de la population, cadastre, registre des entreprises, registre foncier, assurance maladie – de communiquer entre eux de manière sécurisée, chiffrée, signée électroniquement et intégralement journalisée^[35]. Le registre foncier estonien est ainsi et par exemple entièrement numérique et accessible en ligne avec carte d'identité, Mobile-ID ou Smart-ID, sans nécessité de visite en guichet, l'intégralité des accès étant tracée^[36]. L'État estonien considère plus largement que, par principe, un citoyen ne doit pas produire une information qu'une administration détient déjà ; il appartient plutôt à l'administration demandeuse d'aller la chercher. Ce modèle, qui équipe aujourd'hui plus de huit cents registres et bases publiques et privées, a été adopté par la Finlande en 2017 et sert depuis à des échanges transfrontaliers automatisés entre les deux pays.

Le modèle estonien, retenu également (bien que moins fermement) par l'Union européenne au titre du règlement du 2 octobre 2018 établissant un portail numérique unique^[37] fait de la minimisation non une contrainte opposable au traitement administratif, mais plutôt le principe d'organisation de l'administration. La construction française, qui tend à additionner depuis vingt ans des instruments de simplification sans jamais changer fondamentalement la donne, reste fondée sur le modèle inverse : l'utilisateur fournit, l'administration vérifie. Si changer de modèle paraît urgent pour la France, des difficultés demeurent. En effet, le passage d'un modèle à l'autre suppose non seulement une mobilisation technique et donc des moyens, mais également une inflexion politique significative de la relation entre l'État et le citoyen.

^[35] Nordic Institute for Interoperability Solutions, documentation technique X-Road, open-source sous licence MIT, utilisé en production en Estonie depuis 2001 et en Finlande depuis 2017. Le principe du « *once-only* » est rendu opérationnel par l'interconnexion sécurisée de plus de huit cents registres et bases de données publiques et privées.

^[36] V. Ministère estonien de la Justice et des Affaires numériques, communication « Interoperability and Digital Innovation in the Estonian Land Register », 4 juin 2026.

^[37] Règlement (UE) 2018/1724 du Parlement européen et du Conseil du 2 octobre 2018 établissant un portail numérique unique (Single Digital Gateway), précité.

En effet, le passage d'un modèle à l'autre suppose non seulement une mobilisation technique et donc des moyens, mais également une inflexion politique significative de la relation entre l'État et le citoyen.

Rendre la minimisation effective

Le constat dressé dans les développements qui précèdent appelle une réponse publique certaine et proportionnée à la hauteur des enjeux contemporains de cybersécurité. Elle ne saurait se limiter à une énième campagne de sensibilisation ou à l'adoption d'un nouveau guide – ces démarches étant au demeurant nécessaires. Il nous semble que le modèle français doit radicalement évoluer pour endiguer les fuites de données et, surtout, leurs conséquences dramatiques. La réponse doit selon nous mobiliser trois éléments complémentaires.

Collecter moins, sanctionner plus, afficher systématiquement

D'une part, il est temps d'adopter une interdiction nette et effective des collectes manifestement excessives, assortie de la promotion d'une alternative pratique (comme la validation visuelle). L'interdiction étant une disposition négative, il est possible d'imaginer plutôt la promotion d'une obligation d'abstention de collecte, ce qui revient au même.

D'autre part, un régime de sanction automatique à faible seuil, calibré pour corriger les pratiques ordinaires et non pour frapper les manquements les plus graves, doit être imaginé. Le dispositif de contrôle actuel reste insuffisant pour corriger la pathologie décrite. Les sanctions prononcées par la CNIL demeurent peu nombreuses à l'échelle de l'administration française (87 sanctions en 2024, dont une faible part visant des entités publiques ; la plupart portent sur la vidéosurveillance, les enregistrements téléphoniques ou la géolocalisation, non sur les pratiques ordinaires de collecte au guichet). La procédure simplifiée instituée par la loi du 24 janvier 2022 permet désormais au président désigné de la Commission de prononcer, sans débat contradictoire oral, un rappel à l'ordre, une injonction ou une amende administrative plafonnée à 20000 euros^[38]. Ce dispositif va dans le bon sens et a été massivement utilisé en 2024 pour les manquements de type standardisé : il a permis une augmentation significative du nombre total de mesures correctrices^[39]. La procédure reste toutefois trop peu mobilisée pour les manquements de collecte au guichet, et son déclenchement dépend d'une saisine préalable qui, en pratique, n'intervient pas pour les manquements ordinaires que subissent chaque jour des millions d'utilisateurs. Dans la continuité de cette proposition, un canal simple d'alerte, permettant au citoyen de signaler un manquement constaté sans engager une procédure contentieuse, devrait être mis en place.

^[38] Loi n° 2022-52 du 24 janvier 2022 relative à la responsabilité pénale et à la sécurité intérieure, article 33 (création d'une procédure de sanction simplifiée devant la CNIL permettant au président désigné de prononcer, sans débat contradictoire oral, un rappel à l'ordre, une injonction ou une amende administrative plafonnée à 20 000 euros)

^[39] V. la série de délibérations CNIL de sanction en procédure simplifiée visant des manquements à la minimisation des données (vidéosurveillance, enregistrements téléphoniques, géolocalisation), 2024-2026.

Enfin, une véritable visibilité du principe, par l’affichage obligatoire dans tous les lieux d’accueil du public et par une campagne nationale de sensibilisation, reste essentielle pour accompagner les mesures proposées. La formation des agents publics au principe de minimisation reste, à ce propos, très inégale selon les cursus et les filières, et absente de nombreux parcours initiaux et continus de la fonction publique territoriale ; il convient d’y remédier.

Une synthèse des propositions

Les propositions qui suivent s’organisent autour de cinq axes.

Le premier axe interdit la collecte et la numérisation de certaines pièces manifestement excessives, en promouvant la validation visuelle sur le modèle de ce que pratiquent plusieurs États européens ou nord-européens, et institue une nomenclature nationale opposable des pièces strictement nécessaires par type de démarche.

Le deuxième axe propose d’instaurer un régime d’amendes administratives automatiques, à faible seuil et à procédure simplifiée, en cas d’exigence contraire au principe de minimisation.

Le troisième axe propose de rendre le principe visible et compréhensible, par un affichage obligatoire dans tous les lieux d’accueil du public et par une campagne nationale de prévention et de sensibilisation.

Le quatrième axe propose d’accélérer la mise en œuvre effective du principe « dites-le-nous une fois » déjà consacré en droit français, par la généralisation obligatoire de FranceConnect et des interfaces de programmation existantes, par un audit triennal des pratiques, par la publication annuelle par chaque entité d’un rapport de minimisation, et par la mise en place d’un canal simplifié d’alerte à la CNIL accessible depuis chaque guichet.

Le cinquième axe, enfin, veille à ce que la CNIL et les entités publiques appelées à mettre en œuvre ces nouvelles obligations disposent effectivement des moyens budgétaires et humains nécessaires.

Ces propositions, articulées entre elles, visent à transformer la minimisation d’une obligation théorique en une pratique administrative effective, dans le prolongement direct du principe fondateur du RGPD de 2016 et des lois françaises de 2018 et 2022.

DIX PROPOSITIONS POUR UNE MINIMISATION EFFECTIVE

Nous proposons à titre principal d'adopter, par voie législative, une loi relative à la minimisation des données au sein des entités publiques, intégrée à la loi n° 78-17 du 6 janvier 1978 modifiée, créant une nomenclature nationale opposable des pièces strictement nécessaires par type de démarche, un régime d'amendes administratives automatiques en cas d'exigence contraire à la minimisation, une obligation d'affichage et d'information de l'utilisateur dans tout lieu d'accueil du public, et un canal simplifié d'alerte à la Commission nationale de l'informatique et des libertés accessible depuis chaque guichet.

À titre subsidiaire, à défaut d'une telle codification, la publication par circulaire interministérielle d'un référentiel opposable aux administrations centrales, déconcentrées et territoriales, assortie d'une adaptation réglementaire des codes sectoriels concernés, permettrait de progresser à droit constant.

01

Interdire la collecte et la numérisation de certaines pièces manifestement excessives et promouvoir la validation visuelle

Instituer par voie législative, en complément de la loi du 6 janvier 1978 modifiée et du code de la santé publique, l'interdiction de la collecte et de la numérisation par les entités publiques de certains documents dont la seule présentation visuelle à l'agent de guichet suffit à répondre à l'obligation légale de contrôle. Entrent au premier chef dans cette catégorie les pages de vaccination du carnet de santé des enfants pour l'inscription en crèche, en école, en accueil de loisirs ou en centre de vacances, les justificatifs médicaux détaillés en dehors des cas où ils fondent un droit particulier, les documents d'identité des mineurs lorsqu'une alternative existe, et toute pièce dont la collecte ne répond pas à une obligation précise.

Établir une nomenclature nationale opposable des pièces strictement nécessaires par type de démarche

Instituer par décret en Conseil d'État, après avis de la Commission nationale de l'informatique et des libertés et le cas échéant de la Direction interministérielle du numérique, une nomenclature nationale opposable des pièces strictement nécessaires pour chaque type de démarche administrative récurrente : inscription scolaire ou périscolaire, affiliation sociale, inscription en bibliothèque, demande d'aide, inscription universitaire, recrutement, interventions professionnelles, démarche d'état civil, etc. Toute pièce non listée dans la nomenclature pour une démarche donnée ne pourrait être exigée par l'entité publique responsable, sauf dérogation motivée voire autorisée par la CNIL. Cette nomenclature, publiée et régulièrement actualisée, servirait de référence pour l'élaboration des formulaires types, pour la formation des agents de guichet, pour l'audit des pratiques et pour la saisine simplifiée de la CNIL par les usagers.

02

03

Instituer un régime d'amendes administratives automatiques en cas d'exigence contraire au principe de minimisation

Compléter la procédure simplifiée instituée par la loi du 24 janvier 2022 par un régime d'amendes administratives automatiques, prononcées par le président désigné de la CNIL sans débat contradictoire oral, en cas d'exigence manifestement contraire au principe de minimisation, et dont le montant forfaitaire pourrait être fixé par décret et modulé selon la catégorie d'entité. Le régime viserait notamment les pratiques courantes, comme la demande de pièces non listées dans la nomenclature nationale.

Rendre obligatoire l'affichage visible d'une information sur la minimisation dans tout guichet ou service public

Instituer par décret l'obligation, pour toute entité publique disposant d'un guichet d'accueil ou d'un service en ligne destiné aux usagers, d'afficher de manière visible une information type sur le principe de minimisation des données, sur les droits de l'usager de refuser de fournir une pièce manifestement non nécessaire, et sur les voies de signalement à la CNIL. L'affiche, dont le modèle pourrait être fourni par la CNIL et dont le respect formel relèverait des contrôles ordinaires, préciserait notamment que l'usager peut demander la justification écrite de toute pièce exigée, qu'il dispose d'un droit de rectification, d'opposition, d'effacement et de limitation, et qu'il peut saisir la CNIL depuis un lien ou un code visuel scannable intégré à l'affiche. Une telle obligation d'affichage serait en outre utile pour les agents de guichet, à qui elle rappellerait les limites juridiques de leur demande.

04

05

Rendre obligatoire une formation de tout agent public à un socle minimal de droit des données

Mobiliser les Universités, a minima par circulaire incitant à l'élaboration de programmes, et les autres acteurs de l'enseignement et de la formation comme le Centre national de la fonction publique territoriale, l'Institut national du service public, les instituts régionaux d'administration et les écoles de la fonction publique, en vue de l'établissement rapide d'une formation initiale et continue des agents publics au niveau national. Mobiliser en parallèle le Service d'information du Gouvernement, en lien avec la Commission nationale de l'informatique et des libertés, l'Agence nationale de la sécurité des systèmes d'information et la Direction interministérielle du numérique, pour organiser une campagne nationale de prévention et de sensibilisation aux dangers de la divulgation massive de données dont la collecte est inutile. La campagne, qui devrait associer les acteurs de l'éducation, de la santé et de l'action sociale, aurait pour objectif de faire comprendre à chaque citoyen que chaque donnée inutilement collectée est une donnée inutilement exposée, en s'appuyant sur les exemples récents – France Travail, Viamedis, Almerys, ÉduConnect – pour démontrer l'ampleur des conséquences.

Établir une procédure simplifiée d'alerte à la Commission accessible par code visuel ou lien court

Instituer, en complément du régime d'amendes automatiques institué à la proposition 3, une procédure simplifiée d'alerte accessible à chacun par un code visuel scannable (QR code) ou un lien court intégré à l'affiche réglementaire, permettant à toute personne confrontée à une exigence manifestement contraire au principe de minimisation de la signaler à la CNIL en quelques clics. Le signalement, qui ne constituerait pas en lui-même une plainte, permettrait l'envoi automatisé et non accusatoire d'un rappel des obligations de l'entité concernée voire, le cas échéant et en cas de récidive, d'une mise en demeure à l'entité concernée, publique comme privée. Un seuil de signalements concordants portant sur une même entité ou un même type de pratique pourrait déclencher un contrôle approfondi par les services de la Commission. Ce dispositif, calibré sur le modèle des outils de signalement existants pour d'autres politiques publiques, permettrait un passage à l'échelle du contrôle de la minimisation sans alourdissement proportionné des moyens humains.

06

07

Accélérer la mise en œuvre effective du principe « dites-le nous une fois »

Élargir, par décret en Conseil d'État et après avis de la CNIL, le périmètre des pièces justificatives couvertes par le principe « dites-le nous une fois » consacré par les articles L. 113-12 et L. 114-8 du code des relations entre le public et l'administration, de manière à couvrir l'ensemble des pièces récurrentes des démarches ordinaires. Rendre par ailleurs obligatoire, pour toute entité publique disposant d'un téléservice, le branchement sur FranceConnect pour l'identification et sur les interfaces de programmation API Entreprise et API Particulier pour l'obtention des données déjà détenues par l'administration. Interdire corrélativement, pour les démarches entrant dans le périmètre du principe, toute exigence redondante. Le chiffrage d'économies annuelles potentielles de 320 millions d'euros à généralisation effective (calcul de 2019, à actualiser) constitue sur ce point une marge de manœuvre budgétaire importante pour accompagner la mise à niveau des entités de petite taille.

Rendre obligatoire un audit triennal de minimisation par un tiers indépendant

Pour faire face à l'urgence et à l'ampleur des violations du principe de minimisation, instituer par voie législative une obligation, pour toute entité publique employant plus de cinquante agents ou gérant plus de cinquante mille dossiers d'usagers, de faire réaliser tous les trois ans un audit de minimisation par un tiers indépendant certifié selon un référentiel établi par la CNIL. L'audit porterait sur l'inventaire des traitements, sur la liste des pièces exigées pour chaque démarche, sur la durée effective de conservation, sur les suppressions effectivement réalisées, sur l'existence et le fonctionnement des interfaces avec FranceConnect, API Entreprise et API Particulier, et sur la formation effective des agents. Les conclusions de l'audit seraient rendues publiques et transmises à la CNIL. Les manquements graves identifiés déclencheraient automatiquement une procédure de contrôle.

08

09

Imposer un rapport annuel public de minimisation à chaque entité publique

Instituer par décret l'obligation, pour chaque entité publique au sens de la proposition précédente, de publier chaque année un rapport public de minimisation, intégré au rapport d'activité ou au rapport social. Ce rapport comprendrait l'inventaire des catégories de données collectées, la justification de leur nécessité au regard de la nomenclature nationale, la durée effective de conservation, le nombre de dossiers supprimés dans l'année en application du principe de minimisation, les démarches ayant basculé vers un dispositif d'interrogation plutôt que de collecte, les actions de formation menées auprès des agents. Les éléments agrégés pourraient l'objet d'une publication annuelle par la CNIL afin de permettre une comparaison entre entités comparables.

Renforcer les moyens de la CNIL et des entités publiques concernées

Il va sans dire que les propositions qui précèdent ne peuvent s'entendre sans un accompagnement par l'État de la CNIL, dont les missions se trouveraient légèrement alourdies par l'institution du régime d'amendes automatiques, par le traitement des signalements simplifiés et par la supervision des audits triennaux, ainsi que des entités publiques placées dans l'obligation de faire réellement face à leurs obligations. Cet accompagnement pourrait prendre la forme, en loi de finances, d'un abondement spécifique du budget de la Commission permettant le recrutement d'au moins vingt agents dédiés au traitement des signalements, aux contrôles ciblés de minimisation et à la supervision des audits, et d'un fonds de soutien à la mise en conformité à destination des communes de moins de dix mille habitants et des établissements publics de coopération intercommunale, dont les directions des systèmes d'information manquent fréquemment des ressources techniques et humaines nécessaires pour engager un travail systématique de revue des pratiques de collecte. Les économies annuelles de l'ordre de 320 millions d'euros attendues de la généralisation effective du principe « dites-le nous une fois », rappelées en proposition 7, offrent une marge de manœuvre budgétaire a priori dimensionnée pour un tel accompagnement, sans pression supplémentaire sur les finances publiques.

CONTACT

 contact@observatoire-ethique-publique.com

 07-68-46-86-01

 9 rue Auguste Angellier - 59 000 Lille

 <https://www.observatoireethiquepublique.com/>

