

Décision n° [...] du [...] mettant en demeure [...]

(N° [...])

La Présidente de la Commission nationale de l'informatique et des libertés,

Vu le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des données à caractère personnel et à la libre circulation de ces données ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment son article 20 ;

Vu le décret n° 2019-536 du 29 mai 2019 modifié pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu la délibération n° 2013-175 du 4 juillet 2013 portant adoption du règlement intérieur de la Commission nationale de l'informatique et des libertés ;

Vu la décision n° [...] de la Présidente de la Commission nationale de l'informatique et des libertés de charger le Secrétaire général de procéder ou de faire procéder à une mission de vérification auprès de [...];

Vu les procès-verbaux de contrôle n° [...] ;

Vu les autres pièces du dossier ;

I. Le contexte

La commune de [...] (ci-après « la commune »), dont la mairie est située [...] compte environ [...]habitants. Elle emploie [...] agents et dispose d'un budget de [...] d'euros.

En 1995, la commune a mis en place un système de vidéoprotection en centre-ville dans le cadre d'une politique de lutte contre la délinquance.

En juillet 2019, afin de poursuivre sa politique la commune a développé son système vidéoprotection en installant des caméras supplémentaires.

Au total, 73 caméras ont été installées sur l'ensemble de la commune dont six sont équipées d'un dispositif de lecture automatisée des plaques d'immatriculation (ci-après « LAPI »). Ce dispositif est utilisé afin de répondre aux réquisitions des forces de l'ordre visant à identifier le passage d'un véhicule à partir de son numéro d'immatriculation et ce en dehors de toute convention avec l'Etat.

La commune a procédé aux formalités préalables auprès de la préfecture pour le déploiement puis les modifications du dispositif de vidéoprotection ([...]).

En juin 2020, la Commission nationale de l'informatique et des libertés (ci-après la « CNIL ») a été saisie d'un signalement de la chambre régionale des comptes sur des manquements au

règlement 2016/679 du 27 avril 2016 (ci-après « RGPD ») concernant la diffusion d'un article sur le site web de la commune et le système informatique de la commune.

En application de la décision n° [...] de la Présidente de la CNIL, une délégation de la CNIL a procédé, le [...], à une mission de contrôle sur place auprès de la commune de [...] afin de contrôler la conformité des dispositifs avec l'ensemble des dispositions de la loi Informatique et Libertés du 6 janvier 1978 (ci-après « loi Informatique et Libertés »), du règlement 2016/679 du 27 avril 2016 (ci-après « RGPD »), de la directive 2016/680 du 27 avril 2016 (ci-après « directive police justice ») et des dispositions prévues aux articles L.251-1 et suivants du code de la sécurité intérieure.

Par la suite, la commune a transmis des éléments complémentaires.

Le 1^{er} juillet 2021, la CNIL a procédé à un contrôle sur pièces par un questionnaire portant sur les traitements de données à caractère personnel mis en œuvre par la commune laquelle a apporté une réponse et des pièces complémentaires les 8 et 30 juillet 2021

Le 30 novembre 2021, la CNIL a procédé à un nouveau contrôle sur place portant, plus particulièrement, sur le dispositif de lecture de plaques d'immatriculation.

Les 7 et 9 décembre 2021, la commune a fait parvenir des pièces complémentaires.

II. Sur le manquement relatif au dispositif de lecture automatisée des plaques d'immatriculation (LAPI)

Un manquement à l'obligation de mettre en œuvre un traitement licite et de collecter des données pour des finalités déterminées, explicites et légitimes

L'article 87 de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés prévoit « *Le présent titre s'applique, sans préjudice du titre Ier, aux traitements de données à caractère personnel mis en œuvre, à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces, par toute autorité publique compétente ou tout autre organisme ou entité à qui a été confié, à ces mêmes fins, l'exercice de l'autorité publique et des prérogatives de puissance publique, ci-après dénommés autorité compétente.*

Ces traitements ne sont licites que si et dans la mesure où ils sont nécessaires à l'exécution d'une mission effectuée, pour l'une des finalités énoncées au premier alinéa, par une autorité compétente au sens du même premier alinéa et où sont respectées les dispositions des articles 89 et 90. [...] ».

L'article L.233-1 du code de la sécurité intérieure dispose qu' : « *Afin de prévenir et de réprimer le terrorisme, de faciliter la constatation des infractions s'y rattachant, de faciliter la constatation des infractions criminelles ou liées à la criminalité organisée au sens des articles 706-73 et 706-73-1 du code de procédure pénale, des infractions de vol et de recel de véhicules volés, des infractions de contrebande, d'importation ou d'exportation commises en bande organisée, prévues et réprimées par le dernier alinéa de l'article 414 du code des douanes, ainsi que la constatation, lorsqu'elles portent sur des fonds provenant de ces mêmes infractions, de la réalisation ou de la tentative de réalisation des opérations financières définies à l'article*

415 du même code et afin de permettre le rassemblement des preuves de ces infractions et la recherche de leurs auteurs, les services de police et de gendarmerie nationales et des douanes peuvent mettre en œuvre des dispositifs fixes ou mobiles de contrôle automatisé des données signalétiques des véhicules prenant la photographie de leurs occupants, en tous points appropriés du territoire, en particulier dans les zones frontalières, portuaires ou aéroportuaires ainsi que sur les grands axes de transit national ou international.

L'emploi de tels dispositifs est également possible par les services de police et de gendarmerie nationales, à titre temporaire, pour la préservation de l'ordre public, à l'occasion d'événements particuliers ou de grands rassemblements de personnes, par décision de l'autorité administrative ».

L'article L.233-1-1 du même code dispose qu' « afin de faciliter la constatation des infractions au code de la route, permettre le rassemblement des preuves de ces infractions et la recherche de leurs auteurs ainsi que mettre en œuvre les dispositions de l'article L. 121-4-1 du code de la route, les services de police et de gendarmerie nationales peuvent mettre en œuvre des dispositifs fixes ou mobiles de contrôle automatisé des données signalétiques des véhicules prenant la photographie de leurs occupants, en tous points appropriés du territoire ».

En l'espèce, la commune dispose de six caméras orientées sur la voirie installées à différentes entrées et sorties de la commune, distinctes du dispositif de vidéoprotection équipées d'un lecteur automatique de plaques d'immatriculation. Ce dispositif est mis en œuvre depuis les locaux de la police municipale de la commune.

Lors du contrôle, la délégation a constaté qu'à chaque passage d'un véhicule dans le champ de la caméra une vignette apparaît automatiquement à droite de l'écran de visualisation comprenant :

- une image fixe (image du véhicule) ;
- une suite de caractères alphanumériques (correspondant à la plaque d'immatriculation) ;
- un horodatage ;
- l'identifiant de la caméra.

Ces données sont conservées par la commune avec les enregistrements vidéo correspondants.

La délégation a été informée que ce dispositif, qui est mis en œuvre par la commune et sous sa responsabilité, a pour seule finalité de répondre aux réquisitions des forces de l'ordre, plus précisément, la collecte et la conservation des données relatives aux plaques d'immatriculation des véhicules circulant au sein de la commune de [...] aux fins de mise à disposition de ces données, sur réquisition judiciaire, à la police ou gendarmerie et au parquet.

Or, il résulte des articles précités que les seules autorités compétentes pour utiliser un dispositif LAPI sont les services de police et de gendarmerie nationales et des douanes, de sorte que la commune n'est pas habilitée à mettre en œuvre un tel dispositif. La commune déclare utiliser ce dispositif pour répondre aux réquisitions des services de l'Etat mais le dispositif n'est pas mis en œuvre pour le compte de l'Etat ou dans le cadre d'une convention avec l'Etat. Elle ne peut donc légalement, en tout état de cause, mettre en place ce dispositif.

En outre, l'article L.251-2 du CSI liste les finalités pour lesquelles la transmission et l'enregistrement d'images prises sur la voie publique par le moyen de la vidéoprotection peuvent être mis en œuvre par les autorités publiques compétentes.

Or, mettre les données collectées à la disposition des forces de l'ordre pour l'exercice de ses missions de police judiciaire ne constitue pas une finalité en soi, et la commune n'a pas pu indiquer les finalités précises pour lesquelles les force de l'ordre demandent la mise à disposition des images. Les réquisitions ne paraissent en particulier pas limitées aux infractions listées à l'article L. 251-2 du CSI. Les finalités du dispositif apparaissent donc non déterminées.

Il résulte de ce qui précède qu'un traitement de lecture automatisée des plaques d'immatriculation ne saurait être mis en œuvre licitement par la commune de [...] afin de répondre aux réquisitions des forces de l'ordre.

Ces faits constituent donc une atteinte à l'article 87 de la loi Informatique et Libertés et aux articles L. 233-1 et suivants et L. 251-2 du CSI.

III. Sur les manquements au regard du RGPD

1. Un manquement à l'obligation de définir et de respecter une durée de conservation proportionnée à la finalité du traitement

L'article 5, paragraphe 1, e) du RGPD dispose que « *les données à caractère personnel doivent être [...] conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées* ».

La CNIL rappelle que la durée de conservation des données à caractère personnel doit être déterminée en fonction de la finalité poursuivie par le traitement. Lorsque cette finalité est atteinte, les données sont soit supprimées ou anonymisées, ou font l'objet d'un archivage intermédiaire lorsque leur conservation est nécessaire pour le respect d'obligations légales ou à des fins précontentieuses ou contentieuses notamment. Les données ainsi placées en archivage intermédiaire, le sont pour une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont conservées, conformément aux dispositions en vigueur. Ainsi, après avoir opéré un tri des données pertinentes à archiver, le responsable de traitement doit prévoir, à cet effet, une base de données d'archives dédiée ou une séparation logique dans la base de données active. Cette séparation logique est assurée par la mise en place de mesures techniques et organisationnelles garantissant que seules les personnes ayant un intérêt à traiter les données en raison de leurs fonctions puissent y accéder. Au-delà de ces durées de conservation des données versées en archives intermédiaires, les données à caractère personnel doivent, sauf exception, être supprimées ou anonymisées.

En premier lieu, la commune de [...] a transmis un registre de traitements qui serait en cours d'élaboration dans lequel seuls deux traitements ont une durée de conservation définie (listing des élus, occupation du domaine public). En revanche pour les neuf autres traitements, aucune conservation n'est définie puisqu'il est mentionné au titre de la durée de conservation « *conservation illimitée* » ou « *variable en fonction des documents* ».

En deuxième lieu, s'agissant du traitement relatif au suivi des contentieux, la délégation a constaté que la commune de [...] stocke les différents documents relatifs au contentieux dans des dossiers numériques accessibles par l'explorateur Windows. S'agissant du contentieux

pénal, la délégation a constaté la présence de dossiers numériques classés par année remontant jusqu'à l'année 1997.

La délégation a été informée que la commune n'avait défini aucune politique en matière de conservation de ces documents et données relatives aux contentieux. Toutefois, la commune a indiqué qu'un projet de gestion électronique des documents est en cours et qu'elle est assistée d'un archiviste s'agissant des questions relatives à la gestion des documents au format papier.

En troisième lieu, s'agissant du traitement relatif à la gestion de la vie scolaire, il ressort des constatations effectuées que les données des comptes utilisateurs clôturés de l'application [...] sont versées dans la table d'archives du schéma [...].

La délégation a relevé que le compte utilisateur archivé le plus ancien a été ouvert le 19 avril 2007 et clôturé le 6 avril 2016, l'enfant ayant cessé sa scolarité en 2012.

La délégation a constaté la présence dans les archives de 959 comptes d'utilisateurs inactifs pour lesquels la date de dernière scolarisation est antérieure à 5 ans.

Il apparaît qu'aucune durée de conservation des données archivées n'a été déterminée et que, par conséquent, les données des comptes utilisateurs clôturés sont conservés pour une durée illimitée.

Par conséquent, les données doivent être conservées uniquement le temps nécessaire à la réalisation de finalités déterminées. Les données des utilisateurs ont été collectées afin de permettre le suivi de la scolarité ou des loisirs des enfants de la commune. Dès lors qu'un enfant n'est plus scolarisé ou ne fréquente plus le centre de loisirs depuis une certaine durée (par exemple 2 ans), le compte utilisateur lié devrait être automatiquement archivé puis supprimé.

Or, l'absence de politique définie en matière de conservation des données archivées du logiciel [...] ne permet pas de respecter les exigences de l'article 5-1-e) du RGPD dès lors que ces données sont conservées pour une durée illimitée.

L'ensemble de ces faits constitue donc un manquement à l'article 5§1, e) du RGPD. La commune de [...] devra veiller à définir pour chacun des traitements une durée de conservation des données à caractère personnel strictement nécessaire au regard des finalités poursuivies.

2. Un manquement à l'obligation de mettre en œuvre un registre des activités de traitement

L'article 30 du Règlement prévoit que le responsable de traitement, quel que soit le nombre de ses employés, a l'obligation de tenir un registre des activités de traitement, dès lors que le traitement des données à caractère personnel n'est pas occasionnel.

Dans ce cas, le registre des activités de traitement doit comporter toutes les informations listées à l'article 30.1. du RGPD, à savoir : le nom et les coordonnées du responsable de traitement, de son représentant et du délégué à la protection des données, les finalités du traitement, les catégories de personnes concernées et les catégories de données à caractère personnel, les éventuels transferts de données et dans la mesure du possible, les délais prévus pour l'effacement des données et la description des mesures techniques et organisationnelles mises en œuvre pour garantir un niveau de sécurité des données adapté au risque.

La délégation a relevé que la commune de [...] utilisait de nombreux traitements inhérents à l'activité d'une commune notamment ceux relatifs à l'état civil ou au contentieux.

Or, la commune a transmis à la délégation un registre de traitements qui recense seulement onze traitements.

En outre, les fiches pour chacun de ces traitements sont imprécises notamment en ce qui concerne la durée de conservation des données ou encore la description des mesures techniques et organisationnelles mises en œuvre pour garantir un niveau de sécurité des données adapté au risque.

La commune a indiqué que ce registre était en cours d'élaboration depuis 2019 et devait être finalisé en 2021. Toutefois, la société n'a ni fourni le registre finalisé ni informé de l'état d'avancement de celui-ci.

Ainsi, le registre transmis est incomplet et ne comprend pas toutes les informations requises par l'article 30, paragraphe 1 du RGPD. De nombreux traitements ne sont pas consignés notamment celui relatif aux contentieux ou au domaine scolaire et la plupart des fiches du registre ne contiennent pas les informations requises.

Ces faits constituent un manquement aux obligations de l'article 30 du Règlement. Le responsable de traitement devra donc compléter le registre avec les informations manquantes.

3. Un manquement à l'obligation d'assurer la sécurité et la confidentialité des données

L'article 32 du RGPD prévoit « *le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins [...] des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement* ».

a. Sur les mots de passe

En premier lieu, la délégation a été informée que les mots de passe utilisateurs pour l'ouverture des sessions Windows sur les postes des agents doit être d'une longueur minimale de 8 caractères et comporter une lettre et un chiffre.

En deuxième lieu, les identifiants permettant l'accès au VPN pour l'exercice du télétravail par les agents via l'outil [...] sont définis par la commune. Ils sont constitués du nom d'utilisateur de l'agent, du caractère « @ » suivi du code de photocopieur de l'agent composé uniquement de 5 chiffres. Aucun autre mécanisme d'authentification suffisamment robuste n'est prévu pour accéder à l'outil [...].

En troisième lieu, la délégation a constaté que le mot de passe d'un agent administratif pour se connecter au logiciel de gestion des procédures d'état civil [...] est composé de 6 caractères.

En quatrième lieu, la commune a indiqué que pour accéder à un portail « famille » dans la suite logicielle [...], les administrés dont le compte utilisateur est créé par un agent de la mairie

se voient délivrer un mot de passe composé uniquement de chiffres correspondant au numéro de leur dossier. Ce mot de passe est communiqué à l'utilisateur soit par remise en main propre d'une fiche de création de compte utilisateur, soit par envoi électronique de cette fiche à l'adresse communiquée. Le mot de passe peut ensuite être modifié sans que ce soit une obligation.

En l'espèce, les pratiques précitées ne permettent pas de garantir de façon optimale la sécurité des données traitées. En effet, une authentification reposant sur l'utilisation d'un mot de passe d'un niveau de complexité faible n'est pas suffisant pour garantir une robustesse contre les tentatives de connexion par des tiers non autorisés, et peuvent conduire, ainsi, à une compromission des comptes associés et des données qu'ils contiennent.

La Commission considère que, pour assurer un niveau de sécurité et de confidentialité suffisant, dans l'hypothèse où l'authentification repose uniquement sur un identifiant et un mot de passe, ce dernier doit être composé d'au minimum 12 caractères comprenant des majuscules, des minuscules, des chiffres et des caractères spéciaux à choisir dans une liste d'au moins 37 caractères spéciaux possibles ou bien il doit être d'au minimum 14 caractères comprenant des majuscules, des minuscules et des chiffres, sans caractère spécial obligatoire ou encore lorsqu'il correspond à une phrase fondée sur des mots de la langue française, il doit être composé d'au minimum 7 mots.

A défaut, la Commission considère que permet également d'assurer un niveau de sécurité et de confidentialité suffisant une authentification reposant sur un mot de passe d'une longueur minimum de 8 caractères, composé de 3 catégories de caractères différentes mais accompagnée d'une mesure complémentaire comme, par exemple, la temporisation d'accès au compte après plusieurs échecs (suspension temporaire de l'accès dont la durée augmente à mesure des tentatives), la mise en place d'un mécanisme permettant de se prémunir contre les soumissions automatisées et intensives de tentatives (ex : « captcha ») et/ou le blocage du compte après plusieurs tentatives d'authentification infructueuses (au maximum 10)¹.

Ainsi, pour satisfaire aux recommandations de robustesse des mots de passe et assurer un niveau de sécurité et de confidentialité suffisant lorsque l'authentification repose, comme en l'espèce, uniquement sur un identifiant et un mot de passe, ce dernier devrait être d'une longueur minimum de 12 caractères, et composé de 4 catégories de caractères différentes (lettres majuscules, lettres minuscules, chiffres et caractères spéciaux à choisir dans une liste).

Ces faits constituent donc un manquement à l'article 32 du RGPD. La commune devra donc mettre en œuvre une politique de mot de passe robuste et mettre à jour ou solliciter la mise à jour des outils [...].

b. Sur les systèmes d'information et les applications

D'une part, la délégation a constaté que cinq serveurs hébergés par la commune ([...], le serveur hébergeant l'application de gestion des actes d'état civil [...], le serveur de l'application [...], le serveur de l'application de gestion du parc informatique [...], le serveur de l'application

¹ Délibération n° 2022-100 du 21 juillet 2022 portant adoption d'une recommandation relative aux mots de passe : <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000046432885>

de gestion du protocole (annuaire institutionnel) et le serveur de gestion des badgeuses) utilisaient le système d'exploitation Windows 2003.

Or, ce système d'exploitation qui n'est plus maintenu par son éditeur depuis le 14 juillet 2015 est donc obsolète.

D'autre part, la délégation a été informée que l'application de gestion des actes d'état civil [...] n'était plus maintenue par son éditeur depuis deux ans et est, par conséquent, obsolète.

L'ANSSI recommande que « *Des actions de configuration doivent être menées pour la sécurité du système d'exploitation. Pour cela, il est recommandé de se référer aux guides de sécurité proposés par les éditeurs [...] les points suivants doivent être traités : [...] le durcissement des configurations systèmes ; l'activation de l'ensemble des mécanismes de mise à jour dans le respect des recommandations du chapitre 8 dédié au maintien en condition de sécurité* ». En outre, l'ANSSI précise qu'il convient de respecter le principe de maintien en condition de sécurité.

Or, le fait d'utiliser des systèmes d'exploitation et des applications qui ne sont plus maintenus et ne peuvent être mis à jour contrevient nécessairement au maintien d'un niveau de sécurité suffisant.

Ces faits constituent un manquement à l'article 32 du RGPD. Il appartiendra à la commune de migrer vers des versions maintenues de systèmes d'exploitation ou applications par leurs éditeurs.

c. Sur le réseau

La délégation a constaté que l'ensemble des postes utilisateurs et des serveurs sont connectés à un même réseau sans segmentation.

Or, la CNIL a rappelé que la sécurité des serveurs était une priorité et recommande le cloisonnement réseau qui réduit les impacts en cas de compromission.

De même, l'ANSSI recommande de procéder à un découpage du système d'information. Dans son guide d'hygiène informatique, l'ANSSI précise qu'il est important de segmenter le réseau et mettre en place un cloisonnement entre ces zones.

En l'espèce, aucun mécanisme de cloisonnement du réseau n'a été mis en place par la commune. La compromission d'une machine mettrait ainsi en péril l'ensemble des machines ce qui est contraire à l'obligation de sécurité.

Ces faits constituent donc un manquement à l'article 32 du RGPD. Il appartiendra à la commune de mettre en œuvre un cloisonnement au niveau du réseau afin de limiter la propagation de logiciels malveillants au sein du système d'information.

4. Un manquement à l'obligation de réaliser une analyse d'impact relative à la protection des données

L'article 35 du RGPD dispose que « *lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités*

du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel ».

Le considérant 84 du RGPD précise qu'« afin de mieux garantir le respect du présent règlement lorsque les opérations de traitement sont susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement devrait assumer la responsabilité d'effectuer une analyse d'impact relative à la protection des données pour évaluer, en particulier, l'origine, la nature, la particularité et la gravité de ce risque. Il convient de tenir compte du résultat de cette analyse pour déterminer les mesures appropriées à prendre afin de démontrer que le traitement des données à caractère personnel respecte le présent règlement. Lorsqu'il ressort de l'analyse d'impact relative à la protection des données que les opérations de traitement des données comportent un risque élevé que le responsable du traitement ne peut atténuer en prenant des mesures appropriées compte tenu des techniques disponibles et des coûts liés à leur mise en œuvre, il convient que l'autorité de contrôle soit consultée avant que le traitement n'ait lieu. »

À titre informatif, les lignes directrices du groupe de travail « article 29 » concernant l'analyse d'impact relative à la protection des données et la manière de déterminer si le traitement est susceptible d'engendrer un risque élevé adoptées le 4 octobre 2017, WP248 rev. 01 dressent une liste de neuf critères permettant d'apprécier la notion de « risque élevé » et précisent que « dans la plupart des cas, le responsable du traitement peut considérer qu'un traitement satisfaisant à deux critères nécessite une AIPD ».

Par ailleurs, selon l'article 90 de la loi Informatique et Libertés, « si le traitement est susceptible d'engendrer un risque élevé pour les droits et les libertés des personnes physiques, notamment parce qu'il porte sur des données mentionnées au I de l'article 6, le responsable de traitement effectue une analyse d'impact relative à la protection des données à caractère personnel ».

a. Sur le dispositif de vidéoprotection

La délégation a constaté que la commune de [...] habitants a mis en place un dispositif de vidéoprotection afin de prévenir aux atteintes aux biens et aux personnes, composé de 73 caméras situées notamment aux abords de places, de la mairie et de parkings.

La délégation a été informée que la commune n'a pas réalisé d'analyse d'impact concernant ce dispositif.

Or, celui-ci conduit à la surveillance systématique à grande échelle d'une zone accessible au public, ce qui est susceptible de présenter un risque élevé pour les droits et libertés des personnes physiques.

Dès lors, l'article 90 de la loi Informatique et Libertés imposait à la commune de réaliser une analyse d'impact concernant le dispositif de vidéoprotection déployé.

L'absence de réalisation d'une analyse d'impact constitue un manquement à l'article 90 de la loi Informatique et Libertés.

b. Sur le traitement du centre de l'action sociale de la commune

Le traitement mis en œuvre pour les dossiers des habitants de la commune pris en charge par le centre communal d'action sociale répond aux critères relatifs à la vulnérabilité des personnes et à l'empêchement d'exercer un droit ou de bénéficier d'un service ou d'un contrat définis par les lignes directrices du groupe de travail « article 29 ». En effet, le traitement mis en œuvre par le centre communal d'action sociale en charge de proposer des prestations pour remédier aux situations de précarité ou de difficulté sociale comprend nécessairement des données relatives à des personnes placées dans une situation de précarité sociale notamment en raison de leur âge ou handicap. En outre, le traitement précité et le suivi des personnes viennent à déterminer le bénéfice de certaines prestations ou allocation sociales.

Dès lors, il convient de considérer que l'article 35 du RGPD, éclairé tant par les lignes directrices précitées que par les considérants (et notamment le considérant 84), imposait au responsable de traitement de réaliser une analyse d'impact sur ce traitement.

Ces faits constituent un manquement à l'article 35 du RGPD.

En conséquence, la commune de [...], sise [...], est mise en demeure sous un délai de 6 (six) mois à compter de la notification de la présente décision et sous réserve des mesures qu'elle aurait déjà pu adopter, de :

- **cesser de mettre en œuvre le dispositif LAPI à des fins de réquisitions judiciaires ;**
- **définir et mettre en œuvre une politique de durée de conservation des données collectées qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées, et mettre en œuvre une politique d'archivage intermédiaire des données et une procédure de suppression des données à l'expiration de la durée d'archivage des données ;**
- **mettre en œuvre un registre des traitements comprenant l'exhaustivité des traitements de données mis en œuvre par la commune ;**
- **prendre les mesures de sécurité permettant de préserver la sécurité de ces données et d'empêcher que des tiers non autorisés y aient accès :**
 - mettre en place une politique contraignante relative aux mots de passe, notamment en termes de complexité, un mot de passe est composé de 12 caractères minimum comprenant des majuscules, des minuscules, des chiffres et des caractères spéciaux à choisir dans une liste d'au moins 37 caractères spéciaux possibles.
 - remplacer les logiciels et systèmes d'exploitation non maintenus par des versions maintenues par leurs éditeurs ;
 - mettre en œuvre un cloisonnement au niveau du réseau afin de limiter la propagation de logiciels malveillants au sein du système d'information ;
- **réaliser une analyse d'impact relative à la protection des données concernant les traitements susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes concernées, sur la mise en œuvre du dispositif de vidéoprotection et pour le**

traitement portant sur les dossiers des résidents pris en charge par un centre communal d'action sociale (CCAS) ;

Cette mise en demeure n'appelle pas de réponse de votre part auprès de la CNIL. En revanche, si la persistance ou la réitération des manquements visés dans la mise en demeure était constatée à l'occasion de vérifications ultérieures, je pourrais désigner au sein de la CNIL un rapporteur et saisir la formation restreinte de la CNIL, sans qu'une nouvelle mise en demeure ne vous soit adressée préalablement, afin que soit prononcée, le cas échéant, l'une ou plusieurs des mesures correctrices prévues par les articles 20 et suivants de la loi du 6 janvier 1978.

La Présidente

Marie-Laure DENIS