Chambre Contentieuse

Décision quant au fond 19/2020 du 29 avril 2020

N° de dossier : DOS-2018-05421

Objet : Plainte à l'encontre d'une Ville sur la régularité de la consultation de la photo d'une citoyenne dans le Registre national par un employé communal

La Chambre Contentieuse de l'Autorité de protection des données, constituée de Monsieur Hielke Hijmans, président, et de Messieurs Y. Poullet et C. Boeraeve, membres. L'affaire est reprise dans cette composition.

Vu le 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, et abrogeant la Directive 95/46/CE (Règlement Général sur la Protection des Données), ci-après RGPD;

Vu la Loi du 3 décembre 2017 *portant création de l'Autorité de protection des données* (ci-après LCA);

Vu la Loi du 8 août 1983 *organisant un Registre national des personnes physiques*. ;

Vu le Règlement d'ordre intérieur de l'Autorité de protection des données tel qu'approuvé par la Chambre des représentants le 20 décembre 2018 et publié au Moniteur belge le 15 janvier 2019 ;

Vu les pièces du dossier ;

A pris la décision suivante concernant :

- La plaignante
- Le responsable de traitement (ci-après la défenderesse)

I. Rétroactes de la procédure

Vu la plainte déposée le 2 octobre 2018 par la plaignante auprès de l'Autorité de protection des données ;

Vu la décision du 26 octobre 2018 du Service de première ligne de l'Autorité de protection des données déclarant la plainte recevable et la transmission de celle-ci à la Chambre contentieuse à cette même date ;

Vu la décision prise par la Chambre contentieuse lors de sa séance du 14 novembre 2018 de demander une enquête au Service d'Inspection en application des articles 63,2° et 94, 1° LCA ; Vu la saisine de l'Inspecteur général à cette même date ;

Vu le rapport et procès-verbal d'enquête de l'Inspecteur général transmis le 17 mai 2019 à la Chambre contentieuse ;

Vu la décision prise par la Chambre contentieuse lors de sa séance du 28 mai 2019 de considérer que le dossier était prêt pour traitement quant au fond en vertu des articles 95 § 1er, 1° et 98 LCA ;

Vu la communication, le 29 mai 2019, du rapport et procès-verbal d'enquête de l'Inspecteur général aux parties et l'invitation de la Chambre contentieuse aux parties à faire valoir leurs arguments selon un calendrier établi ; Vu la décision du 19 juillet 2019 de la Chambre contentieuse de remplacer le délai de dépôt ultime des conclusions pour la défenderesse du 19 juillet 2019 par la date du 19 août 2019 ;

Vu les conclusions déposées le 19 août 2019 par les conseils de la défenderesse et le courriel les accompagnant aux termes duquel les conseils de la défenderesse précisent que leur cliente souhaite être entendue en application de l'article 51 du Règlement d'ordre intérieur de l'Autorité de protection des données ;

Vu l'audition lors de la séance du 18 novembre 2019 au cours de laquelle la défenderesse représentée par son conseil a comparu. Au terme de cette audition, la Chambre Contentieuse a décidé de mettre l'affaire en continuation et demandé à la défenderesse de lui communiquer toutes pièces complémentaires qui attesteraient de dernières mesures mises en place depuis la communication de ses conclusions en août 2019 ;

...

Vu le procès-verbal d'audition du 18 novembre 2019 ;

Vu les pièces complémentaires déposées par la défenderesse les 22 et 26 novembre 2019;

Vu le courrier en réponse de la plaignante du 11 décembre 2019 ;

Vu les dernières pièces déposées en réplique par la défenderesse le 14 janvier 2020.

II. Les faits et l'objet de la plainte

Aux termes de sa plainte, la plaignante déclare qu'elle a des doutes quant à la régularité de la consultation de sa photo dans le Registre national en date du 11 mai 2018 par un employé de la défenderesse. Le 27 juin 2019, elle adresse un courriel à l'helpdesk Belpic (SPF Intérieur – Direction générale Institutions et Populations) en ces termes :

> *« Madame, Monsieur,*
> *En consultant mon dossier via IBZ, je constate qu'une consultation en « Code transaction 08 – Consultation photo » a été faite en date du 11/05/2018 à 14h39.*
>
> *Sachant que j'étais en voyage de noce à ce moment-là, je trouve cela assez étrange que quelqu'un consulte ma photo.*
>
> *(….) je sais donc par expérience qu'on ne consulte pas un code transaction 08 sans motif valable. Il s'agit certainement d'un(e) collègue, donc j'aimerais en savoir plus si possible.*
> *(…) ».*

Le 28 juin 2019, l'HelpDesk Belpic lui répond par courriel ce qui suit :

> *« Les membres du personnel des organismes habilités à accéder aux données du Registre national sont tenus au secret professionnel. La consultation abusive de dossier (par ex. à des fins privées) engage leur responsabilité personnelle au niveau disciplinaire, civil et pénal.*
>
> *En cas de suspicion concernant une consultation abusive ou non règlementaire de vos données par un organisme, vous pouvez vous renseigner directement auprès de celui-ci. Les organismes sont en effet tenus d'assurer la traçabilité et l'archivage des consultations réalisées en leur sein et pourront normalement vous fournir des informations concernant la nature de ces consultations.*
>
> *Si la réponse fournie n'est pas satisfaisante ou si vous avez de sérieuses raisons de penser qu'une consultation est abusive, vous avez la possibilité d'introduire une plainte auprès de la*

Commission de la protection de la vie privée (https://www.privacycommission.be/fr) ou d'un tribunal.

Les services du Registre national ne disposent généralement pas d'informations concernant les consultations réalisées par ces instances et ne sont en outre pas habilités à gérer les plaintes ».

Toujours par courriel du 28 juin 2019, la plaignante s'adresse à une ancienne collègue de travail, pour savoir à qui s'adresser sa demande auprès de la défenderesse. Sans réponse, la plaignante réitère sa demande par courriel du 14 août 2019. Par courriel du 29 août 2019, il est répondu à la défenderesse qu'une enquête a été demandée et que la plaignante sera informée du résultat de celle-ci ultérieurement.

La plaignante s'enquiert de la suite réservée à sa demande par courriel du 27 septembre 2019. Par courriel du 27 septembre 2019, il lui est répondu ce qui suit :

« Dag,
Een onderzoek werd opgestart maar leverde geen totale zekerheid op noch at betreft de persoon die uw dossier consulteerde (alleen de foto), noch wat betreft de eventuele motivatie voor de raadpleging.
Er werden geen bekentenissen afgelegd. De feiten werden evenwel geacteerd".

Traduction libre:
« Bonjour,
Une enquête a été ouverte mais n'a pas apporté de certitude absolue ni concernant la personne qui a consulté votre dossier (uniquement la photo) ni la motivation éventuelle de la consultation.
Aucun n'aveu n'a été fait. Toutefois les faits ont été actés ».

Le 2 octobre 2019, la plaignante dépose plainte auprès de l'Autorité de protection des données.

III. Le rapport et procès-verbal d'enquête de l'Inspecteur général

Aux termes de son rapport et procès-verbal d'enquête du 17 mai 2019, l'Inspecteur général dresse le constat suivant :

Constatation 1 : la défenderesse n'a pas été en mesure de pouvoir justifier la consultation litigieuse conformément à l'article 17 de la Loi du 8 août 1983 organisant un registre national

...

des personnes physiques. A cet égard, son registre des consultations n'indique pas la finalité pour laquelle les données du Registre national ont été consultées.

Le rapport fait par ailleurs état du renvoi de la défenderesse à la *Recommandation 07/2017 du 30 août 2017 de la Commission de la protection de la vie privée aux villes et communes concernant l'enregistrement du motif de la consultation du Registre national*. [1] En effet, par courrier du 19 février 2019, s'adressant au Délégué à la Protection des données (DPO) de la défenderesse, l'Inspecteur général demande notamment que lui soit fournie *« une explication des raisons pour lesquelles aucune réponse concrète n'a été donnée à la question du citoyen [lisez la plaignante] (voir la recommandation de la CPVP n° 07/2017 du 30 août 2017 aux villes et communes concernant l'enregistrement du motif de la consultation du Registre national par les membres de leur personnel (CO-AR-2017-013) »*.

La défenderesse indique par courrier en réponse du 29 avril 2019 que le contrôle effectué sur la base de la demande de la plaignante a été effectué en date des 20 et 21 août 2019 par consultation de la journalisation SAPHIR utilisée pour les accès au Registre national. Une demande d'explication a ensuite eu lieu auprès de l'agent sous le nom duquel cette consultation a été enregistrée, soit Monsieur X, employé de la défenderesse.

La défenderesse poursuit en précisant que la raison pour laquelle l'identité de l'agent ayant consulté la photo de la plaignante n'a pas été communiquée est liée à l'absence de certitude absolue quant au fait que cet agent est bel et bien l'auteur de la consultation. Cette absence de certitude absolue est *« due au fait qu'il n'avait au moment de son audition pas le souvenir d'avoir effectué cette consultation et a précisé ne jamais consulter les photos de citoyens au départ du registre National mais uniquement dans l'application Belpic, pour procéder à une comparaison lors de la commande de cartes d'identité. Le motif de la consultation journalisée n'a pas pu être établi »* (Extrait de la lettre de la défenderesse du 29 avril 2019 adressée à l'Inspecteur général de l'APD).

Enfin, toujours dans le cadre de l'inspection, la défenderesse ajoute que plusieurs éléments attestent de sa volonté de renforcer, depuis 2018, la sensibilisation et la responsabilisation des agents auxquels un accès au Registre national est octroyé dans le cadre de leur fonction. Elle précise à cet égard que l'enregistrement systématique de la finalité pour laquelle les données au Registre national sont consultées n'a pas encore été rendu obligatoire. Le dispositif visant à lutter contre les accès non fondés est essentiellement de nature préventive, mais sans exploitation détective de la journalisation des accès, hormis demande d'un citoyen.
Le rapport d'Inspection relève à cet égard que la défenderesse s'engage dans les termes suivants :

[1] Cette recommandation est publiée sur le site de l'Autorité de Protection des Données et l'a été sur le site de la Commission de la protection de la vie privée dès son adoption en août 2017 : https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/recommandation_07_2017.pdf

...

« Une recommandation sera formulée en vue de rendre obligatoire la saisie du motif de consultation. (…). Dès lors une recommandation visant à compléter le dispositif par une couche de nature détective sera également formulée, selon le principe que le motif enregistré dans la journalisation des accès doit pouvoir être corroboré par un élément concret, comme un dossier, une demande, etc. et qu'une vérification par échantillon puisse s'en assurer » (Extrait du rapport d'Inspection – réponse de la défenderesse du 5 avril 2019 – avis du DPO).

IV. L'audition du 18 novembre 2019

Au cours de l'audition qui s'est tenue le 18 novembre 2019, la défenderesse a, par la voix de ses conseils, exposé les arguments qu'elle avait développés dans ses conclusions du 19 août 2019. Plus particulièrement, les conseils de la défenderesse admettent qu'un problème est effectivement survenu lors de la consultation de la photographie de la plaignante. La défenderesse met également en avant le sérieux avec lequel la plainte de la plaignante a été traitée et les mesures qui ont été décidées et ont été mises ou seront prochainement mises en place pour se conformer à l'article 17 de la Loi relative au Registre national.

EN DROIT

V. Quant à la compétence de l'Autorité de protection des données, en particulier la Chambre contentieuse

En application de l'article 4 § 1er LCA, l'Autorité de protection des données (APD) est responsable du contrôle des principes de protection des données contenus dans le RGPD et d'autres lois contenant des dispositions relatives à la protection du traitement des données à caractère personnel dont la Loi du 8 août 1983 *organisant un Registre national des personnes physiques*.

En application de l'article 33 § 1er LCA, la Chambre Contentieuse est l'organe de contentieux administratif de l'APD. Elle est saisie des plaintes que le Service de Première Ligne (SPL) lui transmet en application de l'article 62 § 1er LCA, soit des plaintes recevables. Conformément à l'article 60 alinéa 2 LCA, les plaintes sont recevables si elles sont rédigées dans l'une des langues nationales, contiennent un exposé des faits et les indications nécessaires pour identifier le traitement de données à caractère personnel sur lequel elles portent et qui relèvent de la compétence de l'APD.

Quant à la consultation de la photographie dénoncée par la plaignante, cette consultation date du 11 mai 2018. Elle a donc eu lieu à une date antérieure à l'entrée en application du RGPD. La Chambre Contentieuse n'est donc pas autorisée à en connaître. En effet, la Chambre Contentieuse trouve le fondement légal de sa compétence dans la Loi du 3 décembre 2017 *portant création de l'Autorité de*

protection des données (LCA) dont l'entrée en vigueur a été fixée, sauf exceptions, à la date du 25 mai 2018 (article 110 de la LCA). Si la Chambre Contentieuse est compétente au regard de traitements de données qui, certes, ont débuté avant le 25 mai 2018 mais perdurent aujourd'hui, elle ne l'est pas pour des traitements ponctuels qui seraient intervenus avant le 25 mai 2018, aucune rétroactivité n'ayant été prévue pour l'exercice dans le temps de sa compétence.

En l'occurrence, comme exposé au point III ci-dessus, l'inspection menée consécutivement au dépôt de cette plainte a révélé des manquements postérieurs à la date du 25 mai 2018, dont la Chambre Contentieuse est dès lors habilitée à connaître (voy. le point VI ci-dessous).

VI. Sur les motifs de la décision

A titre liminaire sur la violation des droits de la défense invoquée par la défenderesse

Dans ses conclusions du 19 août 2019, la défenderesse déplore, à titre liminaire, que la plaignante n'ait pas déposé de conclusions (point 10 des conclusions de la défenderesse). Elle ajoute qu'il est impossible, au vu du libellé de la plainte de cette dernière, de saisir de manière exhaustive ce qui lui est reproché et plus précisément les dispositions légales qui auraient été violées.
Partant, la défenderesse est d'avis que ses droits de la défense n'ont, en l'espèce, pas été respectés.
Au cours de l'audition du 18 novembre 2019, la défenderesse a répété ses regrets et griefs à cet égard.

La Chambre Contentieuse est par ailleurs d'avis qu'il ne peut être exigé d'un plaignant qu'il identifie de manière claire, précise et exhaustive les dispositions légales à l'appui desquelles il dépose sa plainte. Ce travail de qualification des faits - constitutifs de manquement(s) à la règlementation en vigueur en matière de protection des données à caractère personnel le cas échéant - revient à l'Inspection et à la Chambre Contentieuse. Qu'à cet égard, le courrier du 19 février 2019 de l'Inspecteur général interroge la défenderesse sur les raisons pour lesquelles elle n'a pas respecté la Recommandation 07/2017 laquelle énonce clairement que la mention du motif de la consultation constitue une garantie nécessaire et obligatoire pour accéder au Registre national de manière légitime.

Il ressort du courrier en réponse de la défenderesse du 25 avril 2019, que cette dernière a bien compris ce qui lui était reproché. Le rapport d'Inspection communiqué le 29 mai 2019 à la défenderesse fait encore état de cette recommandation. Enfin, au point 11 de ses conclusions en réplique, la défenderesse, nonobstant sa défense à titre liminaire, indique : « *Nonobstant ce qui précède, deux demandes semblent se dégager de la plainte déposée le 2 octobre 2018 :*

- *L'identité de l'auteur de la consultation du Registre national litigieuse ;*
- *Les motifs de cette consultation, dans la mesure où subsistent dans le chef de la plaignante des doutes quant au lien entre cette consultation et son licenciement, qu'elle qualifie d'abusif* ».

...

La défenderesse se défend ensuite quant à ces griefs dans ses conclusions.

En conclusion, compte tenu de ce qui précède, il ne peut être retenu que les droits de la défense de la défenderesse n'auraient pas été respectés.

*

Sur le nécessaire respect du principe de responsabilité (articles 5 § 2 et 24 du RGPD) et de l'obligation de sécurité (articles 32 du RGPD et 17 de la *Loi organisant un Registre national des personnes physiques*), couplés aux principes de finalité (article 5 § 1 b) du RGPD) et de sécurité (articles 5 § 1 f) du RGPD)

En sa qualité de responsable de traitement, la défenderesse est tenue de mettre en oeuvre les principes de protection des données et doit être en mesure de démontrer que ceux-ci sont respectés (principe de responsabilité – article 5.2. du RGPD). Elle doit par ailleurs, toujours en sa qualité de responsable de traitement, mettre en œuvre toutes les mesures nécessaires à cet effet (article 24 du RGPD). La Chambre Contentieuse insiste, comme elle a déjà eu l'occasion de le rappeler dans de précédentes décisions prises à l'encontre de mandataires publics[2], sur le fait que le secteur public, doit, de manière générale, être vecteur d'exemple dans les mesures qu'il adopte pour garantir le respect du droit fondamental à la protection des données personnelles.

L'article 32 du RGPD (obligation de sécurité) spécifie quant à lui ce qui suit :
« 1. 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, pour les droits et libertés des personnes physiques, le responsable de traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un haut niveau de sécurité adapté au risque, y compris entre autres selon les besoins :

> *(…)*
> *b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement*
>
> *(…)*

[2] Voy Autorité de protection des données, Chambre Contentieuse, Décisions 10/2019 et 11/2019 du 25 novembre 2019 aux termes desquelles la Chambre Contentieuse rappelle que la qualité de mandataire public des responsables de traitement mis en cause aurait dû s'accompagner d'un comportement exemplaire au regard du respect de la législation, en ce compris celle relative à la protection des données personnelles.

d) une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement (…) »[3].

Cet article 32 traduit l'article 5.1.f) du RGPD (Chapitre II-Principes) qui énonce quant à lui le principe d'intégrité et de confidentialité en ces termes :

« Les données à caractère personnel doivent être : (…) f) traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris 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 ».

La sécurité des données personnelles est érigée au rang de principe – ce qui démontre son importance accrue – alors qu'elle n'était pas reprise à l'article 6 de la *Directive 95/46/CE* du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, abrogée par l'entrée en application du RGPD).

Parmi les mesures de sécurité adaptées destinées à garantir la confidentialités des données, un responsable de traitement tel que la défenderesse est nécessairement tenu de mettre en place des mesures de sécurité organisationnelles et techniques qui garantissent un contrôle des accès[4] : en d'autres termes, seules les personnes qui, dans l'exercice de leur fonction propre, ont besoin d'accéder à telle ou telle donnée doivent pouvoir bénéficier des accès nécessaires à cet effet.

La Chambre Contentieuse rappelle à cet égard l'article 5 § 1 b) du RGPD (Chapitre II-Principes) qui consacre le principe de finalité, soit l'exigence que les données soient collectées pour des finalités déterminées, explicites et légitimes et ne soient pas traitées ultérieurement d'une manière incompatible avec ces finalités. A cet égard, la défenderesse est autorisée à consulter le Registre national pour des finalités déterminées conformément à la Loi du 8 août 1983 *organisant un Registre national des personnes physiques*.

---

[3] C'est la Chambre Contentieuse qui souligne.

[4] Voy. notamment les Mesures de référence en matière de sécurité applicables à tout traitement de données à caractère à personnel édictées par la Commission de la protection de la vie privée :

https://www.autoriteprotectiondonnees.be/lexique/mesures-de-reference

Sécurisation logique des accès
L'organisme doit s'assurer que les données à caractère personnel ne soient accessibles, conformément à leur classification, qu'aux personnes et aux applications qui en ont explicitement l'autorisation.
Il maintiendra à jour une liste actualisée des différentes personnes habilitées à accéder et traiter ces données et de leurs pouvoirs respectifs (création, consultation, modification, destruction).
Ces différentes autorisations doivent être traduites en dispositifs techniques et contrôles d'accès aux différents éléments informatiques (programmes, procédures, éléments de stockage, équipements de télécommunication, etc.) intervenant dans le traitement des données à caractère personnel.
Ces dispositions techniques doivent inclure les activités en amont (développement applicatif) et en aval (gestion des exemplaires de sauvegarde).
Si le niveau de sécurité l'impose, l'identification des intervenants sera complétée par une procédure d'authentification.

...

Le responsable de traitement doit donc s'assurer que les données à caractère personnel ne sont accessibles qu'aux personnes et aux applications qui en ont explicitement l'autorisation. Il convient d'attribuer à chaque personne son propre compte et l'accès aux données à caractère personnel devrait être exclusivement autorisé en appliquant les principes du besoin d'en connaître. Ces personnes devraient uniquement avoir accès à la fonctionnalité ou aux données dont elles ont besoin aux fins de l'exécution des tâches qui leur sont dévolues et ce, dans le respect du principe de finalité.

Dans sa Recommandation 03/2017 à laquelle renvoie par ailleurs l'Inspecteur général, la Commission de la protection de la vie privée (CPVP) à l'époque, énonce que le principe de responsabilité (articles 5.2. et 24 du RGPD) rappelé ci-dessus « implique donc non seulement que le responsable de traitement respecte les dispositions du RGPD, mais aussi qu'il puisse le démontrer (…). Il ne suffit pas de prendre les mesures techniques et organisationnelles appropriées, selon les termes du Règlement ; cela doit aussi se faire d'une façon transparente et traçable qui permette, en cas de contrôle régulier, d'apporter la preuve des garanties appliquées » (point 16 de la recommandation 07/2017).

La recommandation 01/2017 précise encore que le RGPD, alors en vigueur mais pas encore en application, renforcera les obligations existantes de la LVP [lisez la Loi Vie Privée, soit la Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel], soumettra, dès son entrée en application le 25 mai 2018, les responsables du traitement, en l'occurrence les villes et communes - dont la défenderesse -, au principe de responsabilité et placera également la barre plus haut en ce qui concerne la transparence des traitements (principe de transparence). La dite recommandation conclut que : « la lecture conjointe des dispositions juridiques nationales actuelles et du futur RGPD conduit à conclure dans la présente recommandation que la mention du motif de la consultation constitue une garantie nécessaire et obligatoire pour accéder au Registre national de manière légitime » (point 6 de la recommandation 07/2017)[5].

Il incombe donc à la défenderesse de garantir que l'accès au Registre national demeure limité aux finalités pour lesquelles cet accès a été autorisé. Il lui incombe également d'être en mesure de le démontrer.

Le respect du principe de finalité, pilier de la protection des données, ne peut en effet pas être vérifié si les agents d'une structure telle la défenderesse n'enregistrent pas le motif de la consultation qu'ils opèrent. Il est tout aussi essentiel à cet égard que conformément à l'article 24 du RGPD, la défenderesse dispose d'un mécanisme de contrôle adéquat garantissant que ses agents habilités

[5] C'est la Chambre contentieuse qui souligne.

consultent le Registre national dans le cadre de ces seules finalités. La défenderesse doit disposer d'une application informatique qui permette de légitimer chaque consultation effectuée par son personnel et démontre ainsi que la consultation a eu lieu dans le cadre de l'exercice des tâches du membre du personnel qui a effectué la consultation.

Outre l'article 32 du RGPD, la défenderesse, en sa qualité d'autorité ayant accès au Registre national, est également tenue de respecter les dispositions spécifiques de la Loi du 8 août 1983 *organisant un Registre national des personnes physiques*. Aux termes de l'article 17 de cette loi - entré en vigueur le 23 décembre 2018 - auquel renvoie l'Inspecteur général :

> *« Chaque autorité publique, organisme public ou privé ayant obtenu l'autorisation d'accéder aux informations du Registre national des personnes physiques, en ce compris les services de police, ainsi que ceux de la Justice cités aux articles 5 et 8 doit être en mesure de pouvoir justifier les consultations effectuées, que celles-ci se fassent par un utilisateur individuel ou par un système informatique automatique. A cet effet, afin d'assurer la traçabilité des consultations, chaque utilisateur tient un registre des consultations.*
>
> *Ce registre indique l'identification de l'utilisateur individuel ou du processus ou du système qui a accédé aux données, les données qui ont été consultées, la façon dont elles ont été consultées, à savoir en lecture ou pour modification, la date et l'heure de la consultation ainsi que la finalité pour laquelle les données du Registre national des personnes physiques ont été consultées.*
>
> *(…) ».*[6]

La Chambre Contentieuse a déjà indiqué que les faits à l'origine de la plainte étant antérieurs à la date du 25 mai 2018, elle ne pouvait en connaître. L'inspection – menée du 21 novembre 2018 au 17 mai 2019 - n'en a pas moins révélé que la défenderesse n'avait, de manière générale, pas encore achevé la mise en place les mesures techniques et organisationnelles requises pour se conformer aux articles 5.2., 24 du RGPD (principe de responsabilité) ainsi qu'aux articles 32 du RGPD et 17 de la Loi du 8 août 1983 *organisant un Registre national des personnes physiques (obligation de sécurité), couplés* aux articles 5 § 1 b) et f) du RGPD (principes de finalité et de sécurité), ce que la défenderesse ne conteste pas.

VII. Sur les mesures correctrices et les sanctions

Aux termes de l'article 100 LCA, la Chambre Contentieuse a le pouvoir de :

[6] C'est la Chambre contentieuse qui souligne.

…

1° classer la plainte sans suite ;
2° ordonner le non-lieu ;
3° prononcer une suspension du prononcé ;
4° proposer une transaction ;
5° formuler des avertissements ou des réprimandes ;
6° ordonner de se conformer aux demandes de la personne concernée d'exercer ces droits;
7° ordonner que l'intéressé soit informé du problème de sécurité;
8° ordonner le gel, la limitation ou l'interdiction temporaire ou définitive du traitement;
9° ordonner une mise en conformité du traitement;
10° ordonner la rectification, la restriction ou l'effacement des données et la notification de celles-ci aux récipiendaires des données;
11° ordonner le retrait de l'agréation des organismes de certification;
12° donner des astreintes;
13° donner des amendes administratives;
14° ordonner la suspension des flux transfrontières de données vers un autre Etat ou un organisme international;
15° transmettre le dossier au parquet du Procureur du Roi de Bruxelles, qui l'informe des suites données au dossier;
16° décider au cas par cas de publier ses décisions sur le site internet de l'Autorité de protection des données.

Il importe de contextualiser le manquement aux articles 5.2., 24 du RGPD ainsi qu'aux articles 32 du RGPD et 17 de la loi du 8 août 1983 *organisant un Registre national des personnes physiques,* combinés aux articles 5 § 1 b) et f) du RGPD en vue d'identifier les mesures correctrices les plus adaptées.

La Chambre Contentieuse relève que tant le principe de sécurité (article 5 § 1 f) du RGPD) (et les obligations qui en découlent – article 32 du RGPD) que le principe de finalité (article 5 § 1 b) du RGPD) que le principe de sécurité garantit, sont des principes essentiels du régime de protection mis en place par le RGPD. Le principe de responsabilité énoncé à l'article 5.2. du RGPD et développé à l'article 24 sont au cœur du RGPD et traduisent le changement de paradigme amené par celui-ci, soit un basculement d'un régime qui s'appuyait sur des déclarations et autorisations préalables de l'autorité de contrôle vers une plus grande responsabilisation et responsabilité du responsable de traitement. Le respect de ses obligations par ce dernier et sa capacité à le démontrer n'en sont dès lors que plus importants. Les manquements à ces principes sont constitutifs de manquements graves.

S'agissant du nombre de personnes potentiellement concernées, le Registre national comprend une banque de données d'identification de *toutes* les personnes physiques qui sont inscrites au registre de

...

la population, registre d'attente et registre des étrangers tenus par les communes ou encore les registres consulaires, soit pour la seule défenderesse, plus de XXX inscrits sur un total de 11 millions de personnes inscrites au Registre national.

L'ampleur des opérations effectuées dans le Registre national par les villes et communes telles la défenderesse ne peut par ailleurs modérer l'obligation de prévoir un mécanisme garantissant le respect des finalités pour lesquelles les données du registre national peuvent être accédées via l'indication du motif de cette consultation ni l'exigence d'un contrôle effectif. Au contraire, tant l'article 32 que l'article 24 du RGPD prescrivent que la nature des mesures techniques et organisationnelles prises par une entité telle la défenderesse soit proportionnée à la gravité des risques pour les droits et libertés des personnes concernées. Par nature, cette base de données comprenant un certain nombre d'informations – certes limitées – de plus de 11 millions de personnes nécessite un encadrement particulièrement rigoureux, non seulement compte tenu de son ampleur, mas également de par sa vocation même d'enregistrement, de mémorisation et de communication d'informations relatives à l'identification des personnes physiques.

La Chambre Contentieuse relève que dès 2015, le Comité sectoriel du registre national avait apporté des précisions sur l'ampleur exacte de cette obligation de tenir des fichiers de journalisation dans le cadre de l'accès au Registre national par des administrations locales. Dans cette Recommandation, le Comité précise que *« ce traçage doit comprendre l'identification de l'utilisateur individuel ou du processus ou du système qui a accédé à ces données, les données qui ont été accédées, la façon dont elles ont été accédées(en lecture, en modification, …), quand elles ont été accédées ainsi que le motif de cet accès »*.[7] Le Comité recommandait en outre de prévoir un champ obligatoire pour l'enregistrement du motif de l'accès.

La Commission de la protection de la vie privée (CPVP) avait également indiqué à plusieurs reprises, avant même la recommandation 01/2017, que l'enregistrement du motif de la consultation du registre national revêt une importance cruciale.[8]

Certes il s'agissait là de recommandations. Elles témoignent cependant de la préoccupation majeure exprimée de longue date et des recommandations à mettre un tel mécanisme en place bien avant l'entrée en application du RGPD. En d'autres termes, la question n'était pas neuve et la défenderesse, de par sa qualité, ne pouvait les ignorer.

[7] Recommandation 01/2015 du Comité sectoriel du Registre national aux communes et administrations locales relative à la sécurité de l'information, devant encadrer leurs accès au registre national et traitements consécutifs des données du Registre national, 18 février 2015, points 44-49.

[8] Voy. le point 23 de la Recommandation 01/2017 déjà citée et les références mentionnées.

La Chambre Contentieuse relève également que, tant en cours d'inspection que dans ses conclusions, la défenderesse expose les différentes décisions prises pour se conformer à ses obligations de sécurité destinées à rencontrer les exigences du RGPD et de la Loi du 3 août 1983 *organisant un Registre national des personnes physiques*. Ces décisions sont attestées par différentes pièces du dossier telles que la documentation interne relative à l'accès au registre national, la désignation et le travail du délégué à la protection des données (DPO) (avis du 5 avril 2019) ainsi qu'une recommandation du 25 avril 2019 (acceptée le 6 mai 2019) visant à rendre obligatoire la saisine du motif de consultation avec une implémentation prévue dans le courant du dernier trimestre de 2019.[9] La Chambre Contentieuse relève que ces documents et décisions ont pour la plupart été adoptés en cours d'inspection.

Il ressort en outre des pièces communiquées par la défenderesse dans le cadre de la mise en continuation décidée par la Chambre Contentieuse à l'issue de l'audition du 18 novembre 2019 que le travail de mise en œuvre de la recommandation du DPO de rendre obligatoire, dans toute application au Registre national, la saisie par l'utilisateur de la finalité pour laquelle les données du registre national sont consultées (en plus des autres données à consigner et ce, conformément à l'article 17 de la loi Registre national du 8 août 1983) s'est effectivement poursuivi dans le courant du dernier trimestre 2019 (procès-verbal de réunion « Accès au Registre national du 16 septembre 2019 »).

Il résulte également des pièces du dossier que des recommandations ont été formulées par le DPO de la défenderesse en matière de *contrôle* des accès au Registre national (extrait du procès-verbal de réunion « Accès au Registre national du 16 septembre 2019 »).

La Chambre Contentieuse constate par ailleurs que dans le courant du mois d'octobre 2019, le suivi des recommandations du DPO s'est notamment traduit par l'identification des motifs de consultation pour chacun des groupes ayant accès au registre national et leur introduction dans «SAPHIR ».

La Chambre Contentieuse constate également que par courriel du 22 novembre 2019 libellé « Important RGPD SAPHIR – Consultation RN : nouvelle procédure », la défenderesse a adressé à ses agents un courriel aux termes duquel son DPO les informe qu'une procédure est mise place laquelle comprendra désormais le choix d'un motif de consultation avant toute consultation du Registre national d'un citoyen. Dans l'application Saphir, une liste déroulante reprenant une série de motifs de consultation relatifs aux matières respectives des membres du personnel concerné apparaîtra lors de toute demande de consultation du Registre national. Aux termes de cette procédure, le personnel devra sélectionner la finalité correspondante au type de dossier traité.

[9] Voy. la pièce « réunion accès au registre national du 3 mai 2019 » de la défenderesse

La Chambre Contentieuse constate encore que par courriel du même 22 novembre 2019, la défenderesse a communiqué à ses correspondants informatiques un message aux termes duquel un contrôle périodique (trimestriel) et systématique des accès attribués est mis en place : un listing reprenant le nom, prénom ainsi que le groupe d'accès associé pour chaque agent repris dans la base de données « Users Saphir – RN » est établi. Le contrôle demandera confirmation du nom des agents pour lesquels l'accès doit être maintenu. A défaut de réponse, les accès seront systématiquement supprimés.

Outre ces mesures spécifiques relatives à la mention du motif de la consultation du Registre national, la défenderesse a transmis à la Chambre Contentieuse les supports de formation utilisés à l'appui de sessions internes de sensibilisation au RGPD. Elle a également communiqué à la Chambre Contentieuse des échanges de courriels entre son DPO et les responsables de ses différents départements quant à la finalisation des Registre des activités de traitement des données personnelles (article 30.1. du RGPD) ainsi que les Registres en tant que tels pour les activités de traitement de différents départements. La défenderesse indique que l'élaboration de ces registres est également prévue pour les départements restant.

La Chambre Contentieuse prend acte de ces informations et des documents qui lui sont transmis. Elle considère que ceux-ci témoignent d'un certain nombre de démarches entreprises par la défenderesse pour se conformer aux obligations auxquelles elle est tenue en sa qualité de responsable de traitement. Que si la Chambre se réjouit de telles démarches, elle regrette cependant que la défenderesse, consciente de ses obligations de sécurité, n'ait pas exigé de ses agents la tenue manuelle d'un registre des accès et de leurs motifs dans l'attente de solutions informatiques.

De manière générale, la Chambre Contentieuse souligne la bonne collaboration de la défenderesse - certes requise par l'article 31 du RGPD - tant avec l'Inspecteur général qu'avec la Chambre Contentieuse.

En conclusion, au regard des éléments développés ci-dessus propres à cette affaire, la Chambre Contentieuse estime que les faits constatés et le manquement – auquel la défenderesse affirme qu'il a été remédié depuis - aux articles 5.2., 24 du RGPD ainsi qu'aux articles 32 du RGPD et à l'article 17 de la Loi du 8 août 1983 organisant un Registre national des personnes physiques, combinés aux articles 5 § 1 b) et f) du RGPD, justifie qu'au titre de sanction effective, proportionnée et dissuasive une réprimande (article 100 § 1er, 5° LCA), soit prononcée à l'encontre de la défenderesse.

Compte tenu de l'importance de la transparence en ce qui concerne le processus décisionnel et les décisions de la Chambre Contentieuse, cette décision sera publiée sur le site Internet de l'Autorité de protection des données moyennant la suppression des données d'identification directe des parties et des personnes citées, qu'elles soient physiques ou morales.

...

POUR CES MOTIFS,
LA CHAMBRE CONTENTIEUSE

Décide, après délibération, d'adresser à la défenderesse une réprimande sur la base de l'article 100 § 5° de la LCA.

*

En vertu de l'article 108, § 1 LCA, cette décision peut faire l'objet d'un recours auprès de la Cour des marchés dans un délai de 30 jours à compter de sa notification, avec l'Autorité de protection des données en tant que défenderesse.

Hielke Hijmans
Président de la Chambre Contentieuse