Le Comité de sécurité de l'information : illustration d'une incohérence législative

Loick Gérard[1]

Dernière des lois adoptées afin de mettre la législation belge en conformité avec le RPGD, la loi du 5 septembre 2018 a, via diverses modifications apportées aux lois du 15 janvier 1990 et du 15 août 2012, institué un nouvel organe actif dans le champ de la protection des données à caractère personnel : le Comité de sécurité de l'information. Renouant avec le principe des formalités préalables au traitement alors même que le RGPD établit une nouvelle philosophie basée sur la responsabilisation des acteurs du traitement, le Comité de sécurité de l'information suscite le questionnement tant en ce qui concerne l'opportunité de sa création, qu'en ce qui concerne ses missions et son statut.

Last of the laws adopted in order to bring the Belgian legislation in conformity with the GDPR, the Law of September 5th, 2018 has, via various modifications brought to the laws of January 15th, 1990 and of August 15th, 2012, instituted a new entity active in the field of personal data protection: the Information Security Committee. Reviving the principle of pre-treatment formalities even though the GDPR establishes a new philosophy based on the accountability of data controllers and data processors, the Information Security Committee raises issues regarding the appropriateness of its creation as well as its missions and its status.

I. INTRODUCTION

Avant d'entamer l'étude du Comité de sécurité de l'information, il convient d'introduire le sujet en examinant le principe d'*accountability* instauré par les articles 5, § 2, et 24 du RGPD[2] et les conséquences de son application dans l'ordre juridique interne.

A. Le principe d'*accountability*

Le principe de responsabilité, plus connu dans la littérature sous sa dénomination anglaise d'*accountability*, tend à mettre les acteurs du traitement de données – et en particulier les responsables du traitement – face à leurs responsabilités. En application de ce principe, les responsables du traitement doivent non seulement respecter l'ensemble des obligations et principes fixés par le RGPD mais également être en mesure de démontrer le respect de ceux-ci[3].

[1] Assistant à l'UNamur, chercheur au CRIDS.

[2] 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, *J.O.U.E.*, L. 119, 4 mai 2016.

[3] Voy. C. de Terwangne, K. Rosier et B. Losdyck, « Lignes de force du nouveau règlement relatif à la protection des données à caractère personnel », *R.D.T.I.*, n° 62/2016, p. 28 ; voy. également https://www.autori-

Mettant l'accent sur la responsabilité des acteurs du traitement, le principe d'*accountability* incite également à la suppression des formalités préalables au traitement[4]. À titre d'exemple, c'est en s'appuyant sur le principe de responsabilité que le législateur européen a remplacé l'obligation de déclaration préalable des traitements auprès de l'autorité de contrôle par l'obligation pour les responsables du traitement et sous-traitants de tenir un registre des activités de traitement[5].

Au niveau national, l'application la plus visible du principe d'*accountability* par le législateur fédéral réside dans la suppression des comités sectoriels instaurés auprès de la Commission de la protection de la vie privée.

B. La suppression des comités sectoriels[6]

Intégrés – depuis l'entrée en vigueur de la loi du 26 février 2003[7] – à la Commission de la protection de la vie privée, les comités sectoriels étaient des organes dont la principale mission consistait à analyser la légalité des demandes de communication de données détenues par certains secteurs déterminés de l'administration fédérale. Si la légalité de la communication envisagée était établie, le comité compétent adoptait alors une autorisation indiquant « dans des termes généraux, quelles données peuvent être échangées entre qui et dans quelles circonstances »[8].

Au moment de l'adoption de la loi du 3 décembre 2017 portant création de l'Autorité de protection des données[9], la Commission de la protection de la vie privée comportait encore cinq comités sectoriels : le comité sectoriel de la Banque-Carrefour des entreprises, le comité sectoriel du Registre national, le comité de surveillance statistique, le comité sectoriel de la Sécurité sociale et de la Santé, ainsi que le comité sectoriel pour l'Autorité fédérale[10].

Profitant de la nécessaire réforme de la Commission de la protection de la vie privée, le législateur fédéral procéda à la suppression des comités sectoriels par l'intermédiaire de l'ar-

teprotectiondonnees.be/principe-de-responsabilite-accountability.

4 E. Degrave, « Accountability », in *L'ABC du RGPD : Dictionnaire pratique à destination des administrations*, Namur, Union des Villes et Communes de Wallonie, 2018, p. 19. Si la notion d'*accountability* peut être considérée comme une nouveauté issue du RGPD, l'on constate cependant qu'elle s'inscrit dans un mouvement initié dès l'adoption de la directive 95/46/CE qui avait vu une diminution des contrôles *a priori* exercés par les autorités de contrôles au profit d'un renforcement de leurs interventions *a posteriori* (Y. Poullet, « L'autorité de contrôle : "Vues" de Bruxelles », *Revue française d'administration publique*, 89/1999, p. 75).

5 C. de Terwangne, « Les principes relatifs au traitement des données à caractère personnel et à sa licéité », in *Le Règlement Général sur la Protection des Données (RGPD/GDRP) : Analyse approfondie*, Bruxelles, Larcier, 2018, pp. 117-118.

6 Pour une analyse exhaustive de la composition et des missions des comités sectoriels, voy. E. Degrave, *L'E-Gouvernement et la protection de la vie privée : légalité, transparence et contrôle*, Bruxelles, Larcier, 2014, pp. 627-644.

7 Loi du 26 février 2003 modifiant la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel et la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-Carrefour de la sécurité sociale en vue d'aménager le statut et d'étendre les compétences de la Commission de la protection de la vie privée, *M.B.*, 26 juin 2003, p. 34416.

8 Projet de loi relatif à l'institution et à l'organisation d'une Banque-Carrefour de la sécurité sociale, Commentaire de l'article 15, *Doc. parl.*, Ch. repr., sess. ord. 1988-1989, n° 899/1, p. 22.

9 Loi du 3 décembre 2017 portant création de l'Autorité de protection des données, *M.B.*, 10 janvier 2018, p. 989.

10 Sont omis de cette énumération : le comité de surveillance sectoriel Phenix, supprimé par l'article 29 de la loi du 12 mai 2014 portant modification et coordination de diverses lois en matière de justice (II) ; ainsi que le comité sectoriel « public sector information » créé par l'article 22 de la loi du 4 mai 2016 relative à la réutilisation des informations du secteur public mais qui ne fut jamais mis en place, faute d'adoption de mesures d'exécution par le Roi.

ticle 109 de la loi du 3 décembre 2017[11]. À cette occasion, le législateur a mis en exergue trois arguments qui justifient selon lui la suppression des comités sectoriels[12].

Premièrement, le cadre légal instituant les comités sectoriels a été considéré comme lacunaire. En effet, si celui-ci définissait la composition des comités, il restait muet concernant leurs compétences et les procédures à suivre pour leur soumettre une demande d'autorisation.

Deuxièmement, l'intégration des comités sectoriels à la Commission de la protection de la vie privée immunisait les autorisations octroyées par ceux-ci à tout contrôle de légalité. En premier lieu car un contrôle de ces autorisations par la Commission aurait été complexe, sous peine de voir celle-ci se prononcer sur des décisions prises par ses propres organes. Ensuite, car l'incertitude entourant le statut de la Commission rendait impossible ou à tout le moins hasardeux l'introduction d'un recours en annulation devant le Conseil d'État[13]. On souligne à cette occasion que l'absence de voies de recours ouvertes contre les décisions des comités sectoriels s'inscrivait en contravention avec l'article 28, § 3, de la directive 95/46[14], lequel précisait que : « Les décisions de l'autorité de contrôle faisant grief peuvent faire l'objet d'un recours juridictionnel ».

Enfin, le législateur a tiré un troisième argument de l'apparente impossibilité de déceler un courant jurisprudentiel cohérent au sein de la multitude de décisions prises par les comités sectoriels. Si cette impossibilité nous semble être une conséquence directe de l'absence de règles délimitant précisément le pouvoir d'appréciation reconnu aux comités sectoriels dans l'exercice de leur mission[15], le législateur y a vu le résultat du « jargon » utilisé dans les délibérations et du caractère insatisfaisant du moteur de recherche permettant de naviguer entre celles-ci.

On note avec étonnement qu'aucun des trois arguments mis en avant par le législateur ne se rattache, de près ou de loin, au principe d'*accountability*. Il nous semble cependant que la suppression d'organes dont la mission principale était d'autoriser préalablement certaines communications de données à caractère personnel s'apparente bel et bien à la suppression d'une démarche de contrôle préalable au traitement. Cette analyse apparaît renforcée par la création, quelques mois plus tard, d'un nouvel outil venant encadrer les communications de données provenant d'autorités fédérales.

C. Les protocoles d'échange de données

La loi du 30 juillet 2018[16] crée, par son article 20, un nouvel outil nommé protocole. Le protocole prend la forme d'un document écrit qui doit,

11 Article abrogeant les chapitres VII et VII*bis* de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.

12 Projet de loi portant création de l'Autorité de protection des données, Rapport fait au nom de la Commission de la justice par M. Egbert Lachaert, *Doc. parl.*, Ch. repr., sess. ord. 2017-2018, n° 2648/6, pp. 6-7.

13 Sur ce point, voy. E. Degrave, « La Commission de la protection de la vie privée : un organisme invincible ? », obs. sous Cour administrative du Grand-Duché du Luxembourg, 12 juillet 2005, *R.D.T.I.*, 2006, pp. 225-241.

14 E. Degrave, *L'E-Gouvernement et la protection de la vie privée : légalité, transparence et contrôle*, *op. cit.*, p. 615.

15 Section de législation du Conseil d'État, avis 33.962/2 sur un avant-projet de loi modifiant la loi du 8 août 1983 organisant un Registre national des personnes physiques et la loi du 19 juillet 1991 relative aux registres de la population et aux cartes d'identité et modifiant la loi du 8 août 1983 organisant un Registre national des personnes physiques, p. 7.

16 Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, *M.B.*, 5 septembre 2018, p. 68616.

sauf exception légale, être rédigé lorsqu'une autorité fédérale est amenée à communiquer des données à caractère personnel et que cette communication de données trouve son fondement[17] dans une obligation légale ou dans l'exercice de l'autorité publique. Les protocoles ainsi adoptés sont publiés sur les sites Internet des responsables du traitement impliqués dans la communication de données concernées.

Comme le précise le texte légal, le protocole est directement rédigé par les responsables du traitement – détenteur et destinataire des données – qui participent à la communication de données en cause[18]. C'est ainsi que, à la suite de la suppression des comités sectoriels et conformément au principe d'*accountability*[19], il revient désormais aux acteurs du traitement d'eux-mêmes analyser la légalité, l'ampleur, et les diverses modalités (mesures de sécurité, périodicité du transfert, durée de conservation, …) des transferts de données qu'ils comptent mettre en place.

II. LA CRÉATION DU COMITÉ DE SÉCURITÉ DE L'INFORMATION

Si la suppression des comités sectoriels par la loi du 3 décembre 2017 et la mise en place subséquente des protocoles d'échange de données par la loi du 30 juillet 2018 semblaient démontrer que le législateur fédéral avait pleinement compris les implications du principe d'*accountability*, l'adoption de la loi du 5 septembre 2018[20] modère fortement cette impression.

En effet, de crainte que l'absence d'autorisations préalables freine les échanges de données entre administrations[21], le législateur procède à un improbable rétropédalage en « ressuscitant » le comité sectoriel de la Sécurité sociale et de la Santé et le comité sectoriel pour l'Autorité fédérale, en les renommant chambre « sécurité sociale et santé » et chambre « autorité fédérale », et en les intégrant à un organe nouvellement créé : le Comité de sécurité de l'information.

III. LA COMPOSITION DU COMITÉ DE SÉCURITÉ DE L'INFORMATION

L'article 2 de la loi du 5 septembre 2018 dispose que le Comité de sécurité de l'information est composé de deux chambres : la chambre sécurité sociale et santé, et la chambre autorité fédérale. Pour l'exercice de certaines de ses missions, le Comité peut également siéger en chambres réunies.

La composition de chacune de ces chambres ainsi que le statut de leurs membres sont directement fixés par la loi du 5 septembre 2018.

17 Sa base de licéité.

18 La loi précise en outre que les délégués à la protection des données de l'entité détentrice et de l'entité destinataire doivent obligatoirement remettre un avis préalable à l'adoption du protocole. Si l'un des avis n'est pas suivi par les entités impliquées, cela doit être explicitement mentionné dans les dispositions introductives du protocole.

19 Projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, *Doc. parl.*, Ch. repr., sess. ord. 2017-2018, n° 3126/1, p. 44.

20 Loi du 5 septembre 2018 instituant le comité de sécurité de l'information et modifiant diverses lois concernant la mise en œuvre du 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, *M.B.*, 10 septembre 2018, p. 69589.

21 Projet de loi instituant le comité de sécurité de l'information et modifiant diverses lois concernant la mise en œuvre du 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, Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2017-2018, n° 3185/1, p. 7.

A. Composition des chambres

Le Comité de sécurité de l'information se compose de huit membres effectifs et d'autant de membres suppléants[22]. Afin d'assurer la parité linguistique, quatre membres sont néerlandophones et quatre sont francophones. Ces membres sont répartis entre les deux chambres en fonction de leurs compétences respectives.

La chambre sécurité sociale et santé est composée de six membres : le président du Comité en sa qualité d'expert en sécurité de l'information et en protection de la vie privée, un expert en gestion électronique des identités, deux juristes experts en droit social ou en droit de la santé, et deux médecins experts en matière de gestion de données à caractère personnel relatives à la santé.

La chambre autorité fédérale est composée de quatre membres parmi lesquels : le président du Comité de sécurité de l'information, un expert en sécurité de l'information et en protection de la vie privée, un expert en gestion électronique des identités[23], ainsi qu'un expert en matières financières et fiscales.

Quant aux chambres réunies, elles sont composées de six membres étant entendu qu'un seul juriste expert en droit social ou en droit de la santé et un seul médecin sont autorisés à y siéger.

B. Statut des membres

Le statut des membres du Comité est constitué de quatre types de règles. Des règles relatives aux conditions de nomination et incompatibilités, à la procédure de nomination, aux conditions d'exercice des fonctions, ainsi qu'au statut pécuniaire[24].

1. Conditions de nomination et incompatibilités

Toute personne souhaitant être nommée membre du Comité de sécurité de l'information doit remplir les conditions fixées par l'article 3 de la loi du 5 septembre 2018. Outre les conditions de nationalité et de jouissance des droits civils et politiques, la loi établit diverses incompatibilités de fonction afin de garantir l'indépendance de ses membres.

Premièrement, les membres de parlements, de gouvernements, de cabinets ministériels, ou de l'Autorité de protection des données – en ce compris son personnel – ne peuvent être membres du Comité.

Deuxièmement, les personnes relevant de l'autorité hiérarchique du ministre ayant la sécurité sociale ou la santé publique dans ses fonctions, ou relevant plus largement d'une institution faisant partie du réseau de la Banque-Carrefour de la sécurité sociale ou de la plate-forme eHealth ne peuvent être membres de la chambre sécurité sociale et santé[25].

Enfin, les personnes relevant de l'autorité hiérarchique d'un ministre fédéral ou relevant d'un service public fédéral ne peuvent être membres de la chambre autorité fédérale.

2. Procédure de nomination

Les membres du Comité de sécurité de l'information sont présentés par le Conseil des

22 Notons d'emblée que les membres suppléants doivent répondre aux mêmes conditions que les membres effectifs.

23 Le président du Comité ainsi que le membre expert en gestion électronique des identités sont membres des deux chambres.

24 Ces règles, contenues aux articles 7 et 8 de la loi du 5 septembre 2018, n'appellent pas de commentaires particuliers.

25 On note que l'article 3 est, sur ce point, la copie conforme de l'ancien article 39, § 1er, 1°, de la loi du 15 janvier 1990 qui établissait les incompatibilités applicables aux membres du comité sectoriel de la sécurité sociale et de la santé.

ministres et nommés pour une durée de six ans par la Chambre des représentants.

Si la loi précise que le mandat des membres est renouvelable, elle ne précise cependant pas combien de renouvellements peuvent être accordés[26].

3. Conditions d'exercice des fonctions

Reprenant tel quel le texte qui était applicable aux membres de la Commission de la protection de la vie privée[27], l'article 5 de la loi du 5 septembre 2018 a pour objectif de préserver l'indépendance des membres du Comité en disposant que ceux-ci ne peuvent recevoir d'instructions de personne et ne peuvent être démis de leur fonction en raison des actes posés et opinions émises dans l'accomplissement de leurs missions.

Ce même article précise également que les membres doivent faire preuve d'objectivité et d'impartialité dans l'exercice de leur fonction, motiver les décisions qu'ils adoptent et respecter l'ensemble des principes de bonne administration.

IV. LES MISSIONS DU COMITÉ DE SÉCURITÉ DE L'INFORMATION

Le Comité de sécurité de l'information est chargé de deux missions principales. La première est identique à celle qui était confiée aux comités sectoriels et consiste à autoriser préalablement certaines communications de données à caractère personnel. La deuxième mission est moins spécifique et consiste en la promotion du respect des législations relatives à la protection des données à caractère personnel.

A. La compétence d'autorisation préalable

Chacune des chambres – en ce compris les chambres réunies – du Comité de sécurité de l'information est chargée d'adopter des délibérations visant à autoriser certaines communications de données. Il ressort des travaux préparatoires de la loi du 5 septembre 2018 que ces délibérations ont « force normative »[28], s'identifient à « des décisions de portée générale contraignante »[29] entre les parties et envers les tiers[30], et doivent obligatoirement être obtenues préalablement à la mise en œuvre de traitements de données à caractère personnel.

Dans l'exercice de sa mission d'autorisation, chaque chambre du Comité se limite à vérifier que la communication de données qui lui est soumise respecte les conditions de licéité, de finalités, de proportionnalité et de sécurité du traitement telles que définies par le RGPD. Ainsi, et contrairement à une crainte qui avait été émise par le Conseil d'État[31], le rôle de la chambre compétente du Comité ne se confond pas avec celui des responsables du traitement car elle ne participe pas à la détermination des finalités et moyens d'un traitement de données mais se borne à évaluer si le traitement, tel qu'envisagé au moment de

26 Article 4 de la loi du 5 septembre 2018.

27 Voy. l'article 24, § 6, de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B.*, 18 mars 1993, p. 5801.

28 Projet de loi instituant le comité de sécurité de l'information […], Commentaire des articles, *Doc. parl.*, Ch. repr., sess. ord. 2017-2018, n° 3185/1, p. 65 ; voy. également le Rapport fait au nom de la Commission des affaires sociales par M. David Clarinval, *Doc. parl.*, Ch. repr., sess. ord. 2017-2018, n° 3185/5, p. 8.

29 Projet de loi instituant le comité de sécurité de l'information […], Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2017-2018, n° 3185/1, p. 6.

30 Articles 46, § 2, de la loi du 15 janvier 1990 et 35/1, § 4, de la loi du 15 août 2012.

31 Projet de loi instituant le comité de sécurité de l'information […], Avis de la section de législation du Conseil d'État n° 63.202/2, *Doc. parl.*, Ch. repr., sess. ord. 2017-2018, n° 3185/1, p. 128.

l'introduction de la demande d'autorisation, respecte les exigences du RGPD.

Toutefois, force est de constater que l'examen préalable de la légalité de certaines communications de données s'apparente à un contrôle préalable qui entre non seulement en contradiction avec le principe de responsabilisation des acteurs du traitement (*accountability*) mis en place par le RGPD, mais également avec le mécanisme du protocole d'échange de données mis en place par le législateur fédéral. Ainsi, en favorisant la responsabilisation des autorités publiques fédérales en leur permettant de conclure des protocoles d'échange de données tout en les déresponsabilisant en soumettant certains de leurs traitements à un contrôle préalable[32], le législateur semble avoir perdu toute notion de cohérence. Et les justifications apportées sur ce point[33] – selon lesquelles les délibérations adoptées par le Comité de sécurité de l'information trouvent leur fondement dans des dispositions du RGPD qui permettent aux États membres d'introduire des réglementations spécifiques applicables aux traitements fondés sur une obligation légale ou sur l'exercice de l'autorité publique[34] ainsi qu'aux traitements portant sur des données génétiques, biométriques, ou de santé[35] – peinent à convaincre tant l'interprétation qui en est faite semble contraire à l'esprit du texte européen[36].

Afin de mieux cerner les limites de la compétence du Comité de sécurité de l'information, les lignes qui suivent sont consacrées à l'étude successive de l'étendue des compétences reconnues à chacune de ses chambres, de la procédure de traitement des demandes d'autorisation, et de la manière dont ces délibérations peuvent être contrôlées.

1. *Étendue des compétences du Comité de sécurité de l'information*

a. *Les communications de données soumises à autorisation de la chambre sécurité sociale et santé*

L'étendue de la compétence d'autorisation de la chambre sécurité sociale et santé est fixée par le nouvel article 15, § 1er, alinéa 1er, de la loi du 15 janvier 1990[37], ainsi que par les nouveaux articles 42 de la loi du 13 décembre 2006 portant dispositions diverses en matière de santé[38] et 11 de la loi du 21 août 2008 relative à l'institution de la plate-forme eHealth[39].

§ 1. La compétence fixée par la loi du 15 janvier 1990

À la lecture de l'article 15, § 1er, alinéa 1er, de la loi, il apparaît qu'une autorisation de la chambre sécurité sociale et santé doit être obtenue préalablement à toute communication de données sociales à caractère personnel effectuée par la Banque-Carrefour de la sécurité sociale ou par une institution de sécurité

32 *Idem*, p. 125.

33 Projet de loi instituant le comité de sécurité de l'information […], Commentaire des articles, *Doc. parl.*, Ch. repr., sess. ord. 2017-2018, n° 3185/1, p. 30.

34 Article 6, § 2, du RGPD.

35 Article 9, § 4, du RGPD.

36 Sur ce point, voy. projet de loi instituant le comité de sécurité de l'information […], Rapport fait au nom de la Commission des affaires sociales par M. David Clarinval, *Doc. parl.*, Ch. repr., sess. ord. 2017-2018, n° 3185/5, pp. 4-10 ; B. Salovic, O. Guerguinov et T. Léonard, « Sous couvert de sécurité, la loi belge viole-t-elle le RGPD ? », 12 septembre 2018, disponible sur : https://www.droit-technologie.org/actualites. *Contra* : Commission de la protection de la vie privée, avis n° 34/2018 du 11 avril 2018, pp. 3-4.

37 Loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-Carrefour de la sécurité sociale, *M.B.*, 22 février 1990, p. 3288.

38 Loi du 13 décembre 2006 portant dispositions diverses en matière de santé, *M.B.*, 22 décembre 2006, p. 73782.

39 Loi du 21 août 2008 relative à l'institution et à l'organisation de la plate-forme eHealth et portant diverses dispositions, *M.B.*, 13 octobre 2008, p. 54454.

sociale[40] à destination d'une autre institution de sécurité sociale[41] ou de toute instance autre qu'un SPF, SPP, ou organisme fédéral d'intérêt public.

À titre d'exemple, c'est sur la base de cette disposition que la Direction générale opérationnelle de l'économie, de la recherche, et de l'emploi (DGO6) du Service public de Wallonie a dû demander des autorisations de la chambre sécurité sociale et santé afin d'obtenir communication de données à caractère personnel détenues par l'ONSS et d'accéder aux registres Banque-Carrefour[42].

Si l'obligation d'obtenir une autorisation pour ce type de communication de données est le principe, notons cependant que celui-ci fait l'objet de quatre exceptions.

Premièrement, l'article 15, § 1er, précise que le Roi peut déterminer les cas dans lesquels les communications de données qu'il vise ne sont pas soumises à autorisation préalable. Cette habilitation, déjà présente dans les versions antérieures de la loi du 15 janvier 1990, a été concrétisée par un arrêté royal du 4 février 1997[43] dont l'article 2 exempte de délibération :

- les communications de données entre une institution de sécurité sociale et son sous-traitant ;
- les communications de données nécessaires à l'accomplissement d'une mission en lien avec la sécurité sociale, effectuées entre institutions de sécurité sociale appartenant au même réseau secondaire[44] ;
- les communications de données nécessaires à l'accomplissement d'une mission en lien avec la sécurité sociale, effectuées entre l'INAMI et le Collège intermutualiste national ou les mutualités ;
- ainsi que les communications portant sur des données d'identification telles que le numéro d'identification de la sécurité sociale, les noms et prénoms, sexe, date de naissance, … lorsqu'elles sont effectuées entre institutions membres du réseau de la Banque-Carrefour de la sécurité sociale.

Deuxièmement, l'article 15, § 1er, alinéa 2, dispose que les communications de données sociales à caractère personnel effectuées entre instances appartenant à une même Région ou Communauté ne requièrent pas de délibération préalable du Comité à condition qu'elles ne s'effectuent pas par le biais de la Banque-Carrefour. Au vu de cette dernière exigence, il faut nécessairement que soit l'instance qui détient les données, soit l'instance qui en demande la communication ait volontairement rejoint le réseau de la Banque-Carrefour de la sécurité sociale[45] dans le respect de la procédure fixée par l'article 18 de la loi du 15 janvier 1990 et l'arrêté royal du 16 janvier 2002[46].

40 Les institutions de sécurité sociale sont largement définies par l'article 2, alinéa 1er, 2°, de la loi du 15 janvier 1990. Un aperçu de ces institutions peut être consulté sur le site web de la BCCS, à l'adresse suivante : https://www.ksz-bcss.fgov.be/fr/a-propos-de-la-bcss/missions/structure-du-reseau.

41 À titre d'exemples d'institutions publiques de sécurité sociale, citons : l'INAMI, l'ONEm, l'ONSS, l'ONVA le SPF Emploi, le SPF Sécurité sociale, ainsi que le SPP Intégration sociale.

42 Comité de sécurité de l'information, Chambre sécurité sociale et santé, délibérations nos 18/144 et 18/136 du 6 novembre 2018.

43 Arrêté royal du 4 février 1997 organisant la communication de données sociales à caractère personnel entre institutions de sécurité sociale, *M.B.*, 3 avril 1997, p. 7788.

44 Tel sera par exemple le cas d'une communication de données entre l'ONEm et un syndicat – tous deux membres du réseau secondaire « institutions de paiement des allocations de chômage » – dans le cadre du paiement d'une allocation de chômage à un affilié.

45 Tel est par exemple le cas du FOREM et de l'AVIQ. Ainsi, une administration de la Région wallonne ne doit pas introduire de demande d'autorisation auprès du Comité de sécurité de l'information pour obtenir communication des données sociales à caractère personnel détenues par ces instances.

46 Arrêté royal du 16 janvier 2002 relatif à l'extension du réseau de la sécurité sociale à certains services publics

Troisièmement, l'article 15, § 2, alinéa 4, exempte d'autorisation les communications de données sociales à caractère personnel effectuées par la Banque-Carrefour de la sécurité sociale ou par une institution de sécurité sociale à destination des archives générales du Royaume ou aux Archives de l'État dans les provinces.

Enfin, l'article 15, § 2, alinéa 6, dispense d'autorisation les communications de données pseudonymysées[47] effectuées par la Banque-Carrefour à certains destinataires limitativement énumérés (les ministres qui ont la sécurité sociale dans leurs attributions, les Chambres législatives, les institutions publiques de sécurité sociale, le Conseil national du Travail, …) à la condition que ces données pseudonymisées soient utilisées par ces destinataires à des fins de connaissance, de conception et de gestion de la protection sociale[48].

Précisons encore que, dans le cadre de sa compétence d'autorisation, et si cela s'avère nécessaire pour assurer l'effectivité de la communication de données sur laquelle elle se prononce, la chambre sécurité sociale et santé peut autoriser les instances concernées à utiliser le numéro d'identification du Registre national[49].

§ 2. La compétence fixée par les lois du 13 décembre 2006 et du 21 août 2008

L'article 42 de la loi du 13 décembre 2006 donne à la chambre sécurité sociale et santé la compétence d'autoriser :

- toute communication de données à caractère personnel relatives à la santé[50-51] ;
- la mise à disposition de tiers de certaines données concernant les hôpitaux ;
- et l'agrégation ainsi que la communication de données détenues par la Fondation Registre du Cancer.

Quant à l'article 11 de la loi du 21 août 2008, il dote la chambre sécurité sociale et santé de la compétence d'autoriser toute communication de données à caractère personnel par ou à destination de la plate-forme eHealth[52].

b. Les communications de données soumises à autorisation de la chambre autorité fédérale

L'étendue de la compétence d'autorisation dont jouit la chambre autorité fédérale est délimitée par le nouvel article 35/1, § 1er, alinéa 1er, de la loi du 15 août 2012 relative à la création d'un intégrateur de service fédéral[53].

et institutions publiques des Communautés et des Régions […], *M.B.*, 6 février 2002, p. 4072.

47 Au sens de l'article 4, 5), du RGPD.

48 Finalités qui sont mentionnées à l'article 5, § 1er, alinéa 1er, de la loi du 15 janvier 1990.

49 Article 15, § 3, de la loi du 15 janvier 1990.

50 Par exemple, une communication de données relatives à la santé effectuée par l'Agence intermutualiste et l'UZ Leuven à destination de la Fondation Registre du Cancer (voy. Comité de sécurité de l'information, Chambre sécurité sociale et santé, délibération n° 18/178 du 3 juillet 2018, modifiée le 2 avril 2019).

51 À l'exception des communications qui sont directement autorisées par une loi ou par arrêté royal, des communications effectuées entre professionnels des soins de santé tenus au secret professionnel et qui concernent leurs patients, et des communications effectuées entre instances d'une même Région ou Communauté et qui ne se font pas à l'intervention de la plate-forme eHealth.

52 À l'exception des communications autorisées ou exemptées d'autorisation par la loi ou par arrêté royal, et des communications de données pseudonymisées lorsque celles-ci sont adressées à certains destinataires limitativement énumérés (ministres et services publics fédéraux qui ont la santé publique ou la sécurité sociale dans leurs attributions, des Chambres législatives, des institutions publiques de sécurité sociale, …) aux fins de réalisation d'études statistiques ou scientifiques.

53 Loi du 15 août 2012 relative à la création et à l'organisation d'un intégrateur de services fédéral, *M.B.*, 29 août 2012, p. 53170.

Le texte légal précise que la chambre autorité fédérale doit être saisie d'une demande d'autorisation pour toute communication de données à caractère personnel effectuée par des services publics et des institutions publiques de l'autorité fédérale à destination de tiers autres que des institutions de sécurité sociale, à la condition que l'instance qui communique les données et l'instance destinataire ne parviennent pas à adopter un protocole d'échange de données tel que défini par l'article 20 de la loi du 30 juillet 2018 ou si l'une de ces instances a fait part de sa volonté de demander une délibération du Comité de sécurité de l'information.

Il apparaît donc que, contrairement à ce qui est prévu pour la chambre sécurité sociale et santé, la compétence de la chambre autorité fédérale n'est que subsidiaire et dépend de la capacité des parties concernées à établir un protocole. Notons toutefois qu'un demandeur de données essuyant un refus de communication de la part d'une autorité publique fédérale ne pourrait voir dans le recours au Comité de sécurité de l'information un moyen de faire pression sur le détenteur des données. La loi précise en effet que la saisine de la chambre autorité fédérale n'est valable que si elle est effectuée par l'ensemble des parties concernées.

À titre d'exemple, c'est sur la base de l'article 35/1, § 1er, alinéa 1er, que le Service Public Régional de Bruxelles – Bruxelles Économie et Emploi a dû demander une autorisation de la chambre autorité fédérale afin d'obtenir communication de données à caractère personnel détenues par la Direction générale Transport routier et Sécurité routière du SPF Mobilité et Transports[54].

Tout comme la chambre sécurité sociale et santé, la chambre autorité fédérale peut, lorsque cela s'avère nécessaire à la réalisation effective de la communication de données qu'elle autorise, permettre aux instances concernées de faire usage du numéro d'identification du Registre national[55].

c. Les communications de données soumises à autorisation des chambres réunies

L'étendue de la compétence d'autorisation des chambres réunies du Comité de sécurité de l'information est fixée par l'article 15, § 2, alinéas 1er et 2, de la loi du 15 janvier 1990, ainsi que par l'article 35/1, § 1er, alinéas 3 et 4, de la loi du 15 août 2012.

Premièrement, les chambres réunies jouissent d'une compétence d'autorisation obligatoire concernant[56] :

- les communications de données sociales à caractère personnel effectuées par une institution de sécurité sociale autre qu'une institution publique de sécurité sociale vers un SPF, SPP, ou organisme fédéral d'intérêt public qui n'est pas une institution de sécurité sociale[57] ;
- et les communications de données effectuées par des services publics et des institutions publiques de l'autorité fédérale vers des institutions de sécurité sociale qui ne sont pas des institutions publiques de sécurité sociale[58].

54 Comité de sécurité de l'information, Chambre autorité fédérale, délibération n° 19/005 du 5 mars 2019.

55 Article 35/1, § 2, de la loi du 15 août 2012.

56 Articles 15, § 2, alinéa 2, de la loi du 15 janvier 1990 et 35/1, § 1er, alinéa 4, de la loi du 15 août 2012.

57 Tel serait par exemple le cas d'une communication de données sociales à caractère personnel effectuée par une mutuelle à destination du SPF Intérieur.

58 Tel est le cas de la communication de données effectuée par la Défense à destination de l'ASBL SIGEDIS (voy. Comité de sécurité de l'information, Chambres réunies, délibération n° 18/194 du 4 décembre 2018).

Deuxièmement, les chambres réunies sont compétentes, mais cette fois de manière subsidiaire, concernant[59] :

– les communications de données sociales à caractère personnel effectuées par la Banque-Carrefour de la sécurité sociale ou par une institution publique de sécurité sociale à destination d'un SPF, SPP, ou organisme fédéral d'intérêt public qui n'est pas une institution de sécurité sociale[60] ;
– et les communications de données à caractère personnel par des services publics et des institutions publiques de l'autorité fédérale à des institutions publiques de sécurité sociale[61].

Comme cela a été précisé s'agissant de la compétence de la chambre autorité fédérale, le caractère résiduaire de la compétence des chambres réunies conditionne sa compétence à l'incapacité des parties concernées d'adopter un protocole d'échange de données ou à la volonté de l'une des parties de saisir le Comité de sécurité de l'information. Comme cela a également été précisé précédemment, la saisine des chambres réunies n'est valable que lorsqu'elle est effectuée par l'ensemble des parties concernées par la communication de données envisagée.

Enfin, on note que ni les textes légaux ni le règlement d'ordre intérieur du Comité ne donnent aux chambres réunies la compétence d'autoriser l'utilisation du numéro de Registre national lorsque celle-ci s'avèrerait nécessaire à la réalisation effective de la communication de données sur laquelle elles se prononcent. Bien qu'il puisse sembler logique que les chambres réunies – en tant qu'émanation des chambres sécurité sociale et santé, et autorité fédérale – jouissent de cette même compétence, la lacune dont se sont rendus coupables le législateur et les auteurs du règlement d'ordre intérieur a pour conséquence de rendre illégale toute autorisation d'utilisation du numéro de Registre national qui serait délivrée par cet organe du Comité de sécurité de l'information.

d. L'extension de la compétence du Comité de sécurité de l'information

De manière surprenante, cela n'étant prévu ni par les lois qui fixent ses compétences, ni par son règlement d'ordre intérieur[62], il ressort de la pratique que le Comité de sécurité de l'information se considère comme compétent pour se prononcer sur la révision de délibérations adoptées par les anciens comités sectoriels Sécurité sociale et Santé, et Autorité fédérale[63].

Si l'attitude du Comité de sécurité de l'information paraît surprenante, force est de constater que celle-ci est la conséquence d'une lacune présente dans l'ordre juridique fédéral. En effet, depuis la suppression des comités sectoriels par la loi du 3 décembre 2017, aucun organe n'est compétent pour se prononcer sur la révision des délibérations adoptées par les comités secto-

59 Articles 15, § 2, alinéa 1er, de la loi du 15 janvier 1990 et 35/1, § 1er, alinéa 3, de la loi du 15 août 2012.

60 Tel est par exemple le cas d'une communication de données sociales à caractère personnel effectuée par l'ONSS à destination du SPF Intérieur (voy. Comité de sécurité de l'information, Chambres réunies, délibération n° 18/094 du 3 juillet 2018, modifiée le 4 décembre 2018).

61 Tel est par exemple le cas d'une communication de données effectuée par le SPF Justice à destination de l'ONEm ou d'une communication de données effectuée par le SPF Finance à destination de FAMIFED (voy. Comité de sécurité de l'information, Chambres réunies, délibérations nos 18/152 et 18/151 du 6 novembre 2018).

62 Le règlement d'ordre intérieur du comité de sécurité de l'information est annexé à l'arrêté royal du 12 novembre 2018 qui y porte approbation, *M.B.*, 27 novembre 2018, p. 90638.

63 Voy. par exemple, la délibération n° 18/152 du 6 novembre 2018 dans laquelle les chambres réunies considèrent le Comité sectoriel pour l'Autorité fédérale comme le « prédécesseur de la Chambre autorité fédérale du Comité de sécurité de l'information » et prolongent un délai fixé par une délibération de celui-ci.

riels. Par conséquent, dans l'état actuel du droit, ces délibérations sont en principe appelées à subsister telles quelles, sans pouvoir faire l'objet de modifications. Une telle situation est incontestablement problématique – la subsistance de délibérations trop restrictives pouvant, par exemple, freiner le partage de données entre administrations – et nécessite urgemment une intervention législative afin d'être solutionnée.

Pour logique qu'elle soit, il n'en demeure pas moins que cette extension de compétence décidée par le Comité de sécurité de l'information se fait au mépris des textes légaux qui fixent ses attributions. En outre, le principe de mutabilité des actes administratifs[64] ne peut être invoqué pour justifier cette extension de compétence concernant des délibérations qui n'ont pas été adoptées par le Comité. En effet, selon le principe de mutabilité, seul l'auteur de l'acte peut ensuite modifier celui-ci[65]. Par conséquent, les délibérations par lesquelles le Comité se prononce sur la révision ou l'extension de délibération adoptées par les comités sectoriels peuvent être considérées comme illégales et faire l'objet d'un recours en annulation devant le Conseil d'État[66].

2. *Procédure de traitement des demandes d'autorisation*

La procédure de traitement des demandes d'autorisation est principalement fixée par le règlement d'ordre intérieur du Comité de sécurité de l'information[67]. Ses dispositions sont, sauf exception, applicables aux trois chambres qui le composent.

En application de l'article 13 du règlement, les demandes de délibération doivent être transmises par voie électronique au Comité de sécurité de l'information[68].

La forme que doivent prendre ces demandes n'est pas fixée par le règlement, lequel renvoie aux modèles de formulaires disponibles sur les sites Internet du SPF Stratégie et Appui, pour les demandes adressées à la chambre autorité fédérale[69], et de la Banque-Carrefour de la sécurité sociale, en ce qui concerne les demandes adressées à la chambre sécurité sociale et santé[70].

La réception de la demande par le Comité de sécurité de l'information donne lieu à l'envoi d'un accusé de réception indiquant le caractère complet ou incomplet de la demande, et invitant, le cas échéant, le demandeur à compléter celle-ci[71]. Le caractère complet d'une demande ne fait toutefois pas obstacle à ce que des informations complémentaires soient réclamées par le Comité en vue de la préparation de la délibération. De plus, et si cela s'avère nécessaire, le président du Comité peut également inviter le demandeur à une audition[72].

64 Ou « loi du changement ».

65 B. Gors, « Du changement à la mutabilité, en passant par l'adaptation continue : retour sur une loi particulière du service public dominant l'action administrative en général », in *Les principes généraux du droit administratif. Actualités et applications pratiques*, Bruxelles, Larcier, 2017, pp. 401-405 ; M. Pâques, « Le retrait : notion, fondement et champ d'application, distinction avec d'autres révisions de l'acte administratif par son auteur », in *La théorie du retrait d'acte administratif*, Bruxelles, Larcier, 2019, pp. 4-7.

66 Sur le recours devant le Conseil d'État, voy. *infra*.

67 L'adoption d'un règlement d'ordre intérieur par le Comité de sécurité de l'information découle de l'habilitation faite aux chambres sécurité sociale et santé et autorité fédérale par les articles 45 de la loi du 15 janvier 1990 et 35/5 de la loi du 15 août 2012.

68 L'adresse de contact n'est pas fixée par le règlement. Après consultation des sites Internet du SPF Stratégie et Appui et de la Banque-Carrefour de la sécurité sociale, il apparaît que les demandes doivent être envoyées à l'adresse csi@mail.fgov.be.

69 dt.bosa.be.

70 www.ksz-bcss.fgov.be.

71 Articles 13 et 14, § 1er, du règlement d'ordre intérieur du Comité de sécurité de l'information.

72 Article 14, § 3, du règlement d'ordre intérieur.

Toute demande complète introduite dans les trente jours calendrier précédant une réunion est en principe traitée lors de la deuxième réunion qui suit l'introduction de la demande[73].

Le demandeur qui souhaite obtenir une autorisation dans un délai raccourci peut invoquer l'urgence. Il lui revient alors de motiver celle-ci. Si l'urgence est jugée fondée, le Comité traite alors la demande en priorité, le cas échéant en recourant à une procédure exclusivement écrite[74].

L'examen de la demande d'autorisation se fait en trois temps et est marqué par une forte implication des membres du personnel des SPF Stratégie et Appui, de la Banque-Carrefour de la sécurité sociale, ou de la plate-forme eHealth. Soulignons d'emblée que, contrairement aux membres du Comité de sécurité de l'information[75], aucun statut particulier ne vient garantir l'indépendance de ces personnes alors même qu'elles sont issues d'institutions pouvant être soumises aux délibérations rendues par le Comité de sécurité de l'information. Au vu de l'importance du rôle qui leur est dévolu, force est de constater que cette situation nuit au caractère indépendant du Comité de sécurité de l'information et favorise la survenance de cas dans lesquels des membres d'une entité contrôlée seront amenés à participer au contrôle de celle-ci[76].

Dans un premier temps, les dossiers à examiner sont préparés par des « collaborateurs » dont l'identité varie en fonction de la chambre compétente du Comité de sécurité de l'information. C'est ainsi que les dossiers qui relèvent de la compétence de la chambre autorité fédérale sont préparés par des collaborateurs du SPF Stratégie et Appui et du SPF Intérieur alors que les dossiers qui relèvent de la compétence de la chambre sécurité sociale et santé sont préparés par des collaborateurs de la Banque-Carrefour de la sécurité sociale et de la plate-forme eHealth[77].

Dans un second temps, des rapports techniques et juridiques succincts « précisant brièvement la matière en question ainsi que les points d'attention particuliers » sont établis. L'identité des instances devant établir ces rapports varie elle aussi en fonction de la chambre compétente et du type de données à caractère personnel concerné. Ainsi, la chambre sécurité sociale et santé recevra rapport de la Banque-Carrefour de la sécurité sociale ou de la plate-forme eHealth[78], la chambre autorité fédérale recevra rapport du SPF Stratégie et Appui[79], et les chambres réunies recevront rapport de la Banque-Carrefour de la sécurité sociale et du SPF Stratégie et Appui[80]. Bien que cela ne soit pas prévu par le législateur, le règlement d'ordre intérieur indique qu'il revient également à ces instances d'annexer un projet de délibération à leurs rapports respectifs.

73 Ainsi, une demande introduite le 2 octobre 2019 – soit plus de 30 jours calendrier avant la réunion du 5 novembre 2019 – sera traitée lors de la réunion du 3 décembre 2019. Le calendrier des réunions est disponible sur le site Internet du SPF Stratégie et Appui.

74 Articles 14, § 2, 15, et 5, § 2, du règlement d'ordre intérieur.

75 Voy. *supra*.

76 Cette situation n'est pas sans rappeler les critiques formulées en leur temps à l'encontre de la composition des comités sectoriels du Registre national et Sécurité sociale et Santé dans lesquels siégeaient des membres de la Banque-carrefour de la sécurité sociale ; voy. E. Degrave, « La Commission de la protection de la vie privée : l'autorité de régulation du secteur des traitements de données à caractère personnel », *Pyramides*, 26/27, 2016, points 55-57.

77 Article 4, § 2, du règlement d'ordre intérieur.

78 Selon que la demande d'autorisation concerne des données sociales ou des données relatives à la santé.

79 Un rapport sera également transmis par le SPF Intérieur si la chambre autorité fédérale est amenée à autoriser l'utilisation du numéro d'identification du Registre national.

80 Articles 42 de la loi du 15 janvier 1990, 35/4 de la loi du 15 août 2012, et 6 du règlement d'ordre intérieur.

Enfin, les délibérations sont adoptées lors des réunions mensuelles tenues par les chambres du Comité de sécurité de l'information[81]. Une délibération ne peut être adoptée par une chambre que si au moins trois de ses membres[82] – outre le président – sont présents[83]. Adoptées de préférence à l'unanimité, les décisions du Comité peuvent être soumises à un vote à main levée et sont alors adoptées à la majorité absolue[84]. Les délibérations ainsi adoptées sont motivées, anonymisées et publiées sur les sites Internet du SPF Stratégie et Appui, de la Banque-Carrefour de la sécurité sociale et de la plate-forme eHealth.

3. *Contrôle des délibérations*

Rompant avec l'immunité dont jouissaient les délibérations des comités sectoriels – qui ne pouvaient faire l'objet d'aucun recours à la suite de l'intégration des comités au sein de la Commission de la protection de la vie privée et des incertitudes entourant le statut de celle-ci[85] –, les délibérations du Comité de sécurité de l'information peuvent faire l'objet d'un contrôle tant par l'Autorité de protection des données que par le Conseil d'État.

a. *Le contrôle par l'Autorité de protection des données*

Le contrôle des délibérations du Comité de sécurité de l'information par l'Autorité de protection des données est explicitement prévu par les nouveaux articles 46, § 2, de la loi du 15 janvier 1990 et 35/1, § 2, de la loi du 15 août 2012[86]. Signalons que cette faculté de contrôle n'était pas initialement prévue par le législateur et a été intégrée à la version finale du texte à la suite des remarques concordantes du Conseil d'État[87] et de la Commission de la protection de la vie privée[88].

Ces textes prévoient que l'Autorité de protection des données peut, à tout moment, vérifier si une délibération du Comité de sécurité de l'information est conforme au droit hiérarchiquement supérieur. À défaut de précisions quant à la manière dont l'Autorité de protection des données peut prendre la décision de contrôler une délibération déterminée, nous en déduisons qu'elle peut le faire soit d'initiative – sur la base de sa mission de contrôle et d'enquête sur l'application du RGPD[89] –, soit suite à l'introduction d'une plainte ou d'une requête par une personne concernée[90].

Dans l'hypothèse où, au terme de son analyse, l'Autorité de protection des données constate qu'une délibération viole les normes supérieures, elle peut demander au Comité de sécurité de l'information de réviser la délibération sur les points qu'elle considère problématiques[91]. Le Comité dispose alors d'un délai de quarante-cinq jours pour soumettre la déli-

81 Articles 7 à 12 du règlement d'ordre intérieur.

82 Trois membres par chambre en ce qui concerne les chambres réunies.

83 Dans les faits, la chambre autorité fédérale – composée de quatre membres dont le président – ne peut donc se prononcer que si l'ensemble de ses membres sont présents.

84 En cas de partage des votes, le vote du président est prépondérant.

85 Voy. *infra*.

86 Sur le plan de la cohérence des législations relatives à l'encadrement des traitements de données à caractère personnel, on ne peut que regretter que, comme l'avait pourtant suggéré la Commission de la protection de la vie privée, cette compétence de l'Autorité de protection des données n'apparaisse pas explicitement dans sa loi organique du 3 décembre 2017 (voy. Commission de la protection de la vie privée, avis n° 34/2018 du 11 avril 2018, p. 4).

87 Projet de loi instituant le comité de sécurité de l'information […], Avis de la section de législation du Conseil d'État n° 63.202/2, *Doc. parl.*, Ch. repr., sess. ord. 2017-2018, n° 3185/1, p. 130.

88 Commission de la protection de la vie privée, avis n° 34/2018 du 11 avril 2018, p. 4.

89 Article 57.1, a) et h), du RGPD.

90 Articles 58 et 60 de la loi du 3 décembre 2017 portant création de l'Autorité de protection des données.

91 La révision vaut exclusivement pour l'avenir.

bération modifiée à l'Autorité. Après réception de la délibération modifiée, l'Autorité jouit elle-même d'un délai de quarante-cinq jours pour accepter ces modifications. À défaut de réaction de sa part dans ce délai, la délibération modifiée est adoptée[92].

Si la mise en place d'un contrôle des délibérations du Comité de sécurité de l'information par l'Autorité de protection des données marque une avancée par rapport au régime antérieur, on s'étonne toutefois de la faiblesse des termes utilisés par le législateur, en particulier lorsqu'il précise que l'Autorité « peut demander au comité de sécurité de l'information […] de reconsidérer sa décision ». Qui plus est, aucune procédure permettant à l'Autorité de protection des données de contraindre le Comité de sécurité de l'information n'est prévue dans l'hypothèse où celui-ci refuserait de modifier une délibération considérée comme illégale. Ces éléments laissent penser que l'effectivité du contrôle mené par l'Autorité de protection des données sera tributaire de la bonne volonté du Comité de sécurité de l'information.

b. Le contrôle par le Conseil d'État

Contrairement à ce qui vient d'être exposé, le contrôle des délibérations du Comité de sécurité de l'information par le Conseil d'État n'est pas explicitement prévu par la loi. Cependant, l'existence d'un recours devant la haute juridiction administrative est mentionnée tant dans l'exposé des motifs – « […] outre les procédures de recours existantes auprès du Conseil d'État » – que dans le commentaire des articles du projet de loi – « les délibérations sont publiées […] et peuvent être contestées par les voies de recours applicables (comme un recours auprès du Conseil d'État) »[93].

Ces indications discrètes mais claires données par le législateur semblent indiquer que le Comité de sécurité de l'information est une autorité administrative[94] – au sens de l'article 14 des lois coordonnées sur le Conseil d'État[95] – dont les délibérations peuvent faire l'objet d'un recours en annulation.

Le recours en annulation, auquel le requérant peut adjoindre une demande de suspension[96], doit être formé dans les soixante jours suivant la publication de la délibération sur Internet[97].

B. La promotion du respect des législations relatives à la protection des données à caractère personnel

Outre sa compétence d'autorisation – qui demeure sa principale attribution – le Comité de sécurité de l'information se voit doté d'autres compétences qui font de lui un organe chargé de promouvoir le respect des législations applicables aux traitements de données à caractère personnel.

Par exemple, c'est à ce titre que la chambre sécurité sociale et santé est chargée de formuler des bonnes pratiques à destination des instances impliquées dans le traitement de

92 Les textes légaux utilisent la formulation suivante : « Dans la mesure où cette dernière ne formule pas de remarques supplémentaires dans un délai de quarante-cinq jours, la délibération modifiée est censée être définitive ». L'utilisation du terme « définitive » est selon nous à proscrire étant donné que celui-ci renvoie, en droit judiciaire, à une décision qui ne peut plus faire l'objet de recours. Or, on ne voit pas quels sont les éléments qui permettraient de soustraire une délibération modifiée à tout contrôle futur par l'Autorité de protection des données.

93 Projet de loi instituant le comité de sécurité de l'information […], *Doc. parl.*, Ch. repr., sess. ord. 2017-2018, n° 3185/1, pp. 10 et 31.

94 Sur la question du statut du Comité de sécurité de l'information, voy. *infra*.

95 Lois sur le Conseil d'État, coordonnées le 12 janvier 1973, *M.B.*, 21 mars 1973, p. 3461.

96 Article 17 des lois coordonnées.

97 Article 4 de l'arrêté du Régent du 23 août 1948 déterminant la procédure devant la section du contentieux administratif du Conseil d'État, *M.B.*, 23 août 1948, p. 6821.

données sociales à caractère personnel ou de données de santé. C'est également en vertu de cette mission qu'elle est chargée de soutenir les délégués à la protection des données en leur fournissant une formation continue adéquate et en formulant des recommandations quant au volet technique de leur mission[98].

Quant à la chambre autorité fédérale, elle est investie de cette même mission de soutien des délégués à la protection des données[99] mais n'est compétente qu'en ce qui concerne les autorités publiques qui ne relèvent pas du champ de compétence de la chambre sécurité sociale et santé[100].

V. LE STATUT DU COMITÉ DE SÉCURITÉ DE L'INFORMATION

Que cela soit ou non volontaire, le législateur n'a pas explicitement fixé le statut du Comité de sécurité de l'information. En effet, tant la loi du 5 septembre 2018 que les lois qu'elle modifie restent muettes quant à la nature de ce nouvel organe. Toutefois, s'il n'a pas clairement défini le statut du Comité, le législateur a cependant affirmé à plusieurs reprises que celui-ci ne peut être considéré comme une autorité de contrôle au sens de l'article 51 du RGPD. C'est entre autres pour éviter cette confusion – et pour ne plus connaître les difficultés issues de l'intégration des comités sectoriels au sein de la Commission de la protection de la vie privée – que les chambres du comité de sécurité de l'information ne sont pas instituées au sein de ladite Autorité[101].

N'étant ni un responsable du traitement, ni une autorité de contrôle, le statut du Comité de sécurité de l'information pose question. En effet, « un tel organisme indépendant, doté d'une autorité normative [n'est] pas expressément prévu dans le RGPD »[102]. Pour l'écrire autrement, l'existence d'un organe tel que le Comité n'avait pas été envisagée par le législateur européen.

Malgré l'absence de statut explicitement fixé par le législateur, fût-il belge ou européen, plusieurs indices incitent à penser que le Comité de sécurité de l'information peut être qualifié d'autorité administrative.

La notion d'autorité administrative n'étant pas définie par le droit positif belge, malgré son utilisation à l'article 14 des lois coordonnées sur le Conseil d'État, il revient à la jurisprudence – et dans une moindre mesure à la doctrine – d'en dresser les contours. Afin de déterminer si une institution est ou non une autorité administrative, il est fait usage de divers critères[103].

98 Article 46, § 1er, de la loi du 15 janvier 1990.

99 Article 35/1, § 3, de la loi du 15 août 2012.

100 La compétence des chambres se limite bien au soutien des délégués à la protection des données. La version initiale du projet de loi donnait au Comité de sécurité de l'information la possibilité d'intervenir lors de la désignation du délégué à la protection des données ou encore d'évaluer sa capacité à exercer correctement ses missions. La disposition projetée avait fait l'objet de critiques formulées tant dans l'avis de la Commission de la protection de la vie privée que dans l'avis du Conseil d'État, en ce qu'elle portait atteinte à l'indépendance du délégué et a été modifiée par le législateur.

101 Projet de loi instituant le comité de sécurité de l'information […], *Doc. parl.*, Ch. repr., sess. ord. 2017-2018, n° 3185/1, pp. 6 et 8 ; projet de loi instituant le comité de sécurité de l'information […], Rapport fait au nom de la Commission des affaires sociales par M. David Clarinval, *Doc. parl.*, Ch. repr., sess. ord. 2017-2018, n° 3185/5, pp. 7-10. Voy. également : Commission de la protection de la vie privée, avis n° 34/2018 du 11 avril 2018, p. 3, en particulier concernant la non-utilisation de l'article 36.5 du RGPD par le législateur.

102 Propos supposément tenus par la Commission européenne, consultée lors de l'élaboration du projet de loi, et rapportés par la ministre des Affaires sociales et de la Santé publique, Projet de loi instituant le comité de sécurité de l'information […], Rapport fait au nom de la Commission des affaires sociales par M. David Clarinval, *Doc. parl.*, Ch. repr., sess. ord. 2017-2018, n° 3185/5, pp. 9-10.

103 Pour un aperçu des questionnements entourant la qualification d'autorité administrative et les critères

Parmi ceux-ci, on distingue classiquement les critères négatifs et les critères positifs.

Selon les critères négatifs, toute institution qui n'appartient ni au pouvoir judiciaire ni au pouvoir législatif est une autorité administrative. Si la non-appartenance du Comité de sécurité de l'information au pouvoir judiciaire ne fait aucun doute, son appartenance au pouvoir législatif peut poser question. On note cependant que l'intervention de la Chambre des représentants dans l'organisation du Comité se limite à la nomination des membres qui le composent. *A contrario*, l'assemblée n'intervient ni dans la fixation du budget ni dans l'établissement du règlement d'ordre intérieur du Comité. En outre, et il s'agit selon nous d'un argument prépondérant, aucune disposition légale analogue à l'article 23 de la loi du 8 décembre 1992 n'indique que le Comité de sécurité de l'information est « institué auprès de la Chambre des représentants »[104].

Concernant les critères positifs, on distingue les critères organiques et les critères fonctionnels.

En application des critères organiques, une autorité administrative est une institution créée par ou en vertu d'une loi et dont le fonctionnement est contrôlé par les pouvoirs publics. Si le Comité de sécurité de l'information est bien créé par une loi, la réalité du contrôle qu'exercent sur lui les pouvoirs publics pose question. En effet, si l'indépendance dont bénéficient les membres du Comité tend, selon le Conseil d'État, à soustraire leurs décisions à tout « contrôle hiérarchique de tutelle de la part du pouvoir exécutif »[105], au moins cinq éléments attestent selon nous l'existence d'un contrôle effectif par le pouvoir exécutif fédéral.

Premièrement, le règlement d'ordre intérieur du Comité de sécurité de l'information est ratifié par un acte du pouvoir exécutif, à savoir un arrêté royal. Deuxièmement, les frais de fonctionnement du Comité de sécurité de l'information, en ce compris les indemnités allouées à ses membres, sont à charge du SPF Stratégie et Appui, de la Banque-Carrefour de la sécurité sociale et de la plate-forme eHealth[106]. Troisièmement, les chambres du Comité siègent respectivement dans les locaux du SPF Stratégie et Appui et de la Banque-Carrefour, lesquels mettent à leur disposition les bureaux, matériels et personnel spécialisé nécessaires à leur fonctionnement[107]. Quatrièmement, le secrétariat du Comité est assuré, en fonction de la chambre compétente, par le SPF Stratégie et Appui ou par la Banque-Carrefour et la plateforme eHealth[108]. Enfin, le personnel du SPF Stratégie et Appui, de la Banque-Carrefour et de la plateforme eHealth, est chargé de préparer les dossiers de demande d'autorisation, d'établir des rapports techniques et juridiques, ainsi que de proposer des projets de délibérations sur les communications de données faisant l'objet de ces demandes.

utilisés, voy. entre autres : J. Salmon, J. Jaumotte et E. Thibaut, *Le Conseil d'État de Belgique, Volume 1*, Bruxelles, Bruylant, 2012, pp. 430-472 ; Y. Mossoux, « La notion d'autorité administrative », in *La publicité de l'administration*, Bruxelles, Bruylant, 2014, pp. 58-67 ; J. Duval et C. Dubois, « Autorité administrative : à la recherche de l'imperium ou d'autres critères ? », *A.P.T.*, 2014, n° 3, pp. 334-340 ; P. Goffaux, *Dictionnaire de droit administratif*, 2e éd., Bruxelles, Bruylant, 2016, pp. 94-100 ; M. Pâques, *Principes de contentieux administratif*, Bruxelles, Larcier, 2017, pp. 246-282.

104 Sur l'application des critères négatifs de l'autorité administrative à la Commission de la protection de la vie privée, voy. E. Degrave, *L'E-Gouvernement et la protection de la vie privée : légalité, transparence et contrôle*, *op. cit.*, pp. 606-612.

105 Projet de loi instituant le comité de sécurité de l'information […], Avis de la section de législation du Conseil d'État n° 63.202/2, *Doc. parl.*, Ch. repr., sess. ord. 2017-2018, n° 3185/1, p. 128.

106 Articles 43 et 35/3 des lois du 15 janvier 1990 et du 15 août 2012.

107 Articles 41 et 35/2, mêmes lois.

108 Article 2, alinéa 2, du règlement d'ordre intérieur du Comité de sécurité de l'information.

En application des critères fonctionnels, une autorité administrative est une institution qui exerce une mission d'intérêt public et dont les décisions unilatérales peuvent lier les tiers. Ces critères sont remplis en ce qui concerne le Comité de sécurité de l'information : celui-ci exerce bien une mission d'intérêt public lorsqu'il veille au respect de la législation relative à la protection des données à caractère personnel dans le cadre de sa compétence d'autorisation, et les délibérations qu'il adopte sont « contraignantes envers les tiers »[109].

Au vu de ces divers éléments, et en gardant à l'esprit les indications du législateur selon lesquelles les délibérations du Comité de sécurité de l'information peuvent faire l'objet d'un recours devant le Conseil d'État, force est de constater que le Comité de sécurité de l'information doit être considéré comme une autorité administrative au sens de l'article 14 des lois coordonnées sur le Conseil d'État.

VI. CONCLUSION

Instauré par une loi adoptée dans l'urgence[110], moins d'un mois sépare la date du dépôt du projet de loi (le 20 juin 2018) de la date de son adoption (le 19 juillet 2018), le Comité de sécurité de l'information est le miroir de l'apparente légèreté avec laquelle le législateur s'est attelé à l'implémentation des principes et obligations issus du RGPD dans l'ordre juridique national.

Ainsi, s'il a dans un premier temps donné l'illusion de saisir l'essence du principe d'*accountability* en remplaçant la formalité préalable de l'autorisation par les comités sectoriels par le mécanisme du protocole d'échange de données, il a ensuite fait montre de son incohérence en rétablissant ce même préalable. Le constat est d'autant plus frappant lorsque l'on prête attention aux dates : tant la loi du 30 juillet 2018 qui crée le protocole que la loi du 5 septembre 2018 qui instaure le Comité de sécurité de l'information ont été adoptées par la Chambre des représentants le 19 juillet 2018. Le législateur a donc, le même jour, adopté deux lois qui mettent en place des mécanismes antagonistes.

Si l'on comprend aisément la volonté du législateur de soumettre à un contrôle préalable les traitements de certains types de données à caractère personnel afin d'assurer la sécurité de ceux-ci, il s'avère cependant que le Comité de sécurité de l'information prend des allures d'organe anachronique à l'heure où le RGPD tend à réduire le recours aux formalités préalables aux traitements dans le but de favoriser une libre circulation des données à caractère personnel[111].

Au milieu de ces critiques, on souligne cependant que l'institution du Comité de sécurité de l'information a été l'occasion pour le législateur de mettre un terme au caractère non contestable des délibérations adoptées en leur temps par les comités sectoriels. Toutefois, la possibilité d'un recours en annulation devant le Conseil d'État n'ayant été reconnue que par l'intermédiaire des travaux préparatoires et non dans le texte légal lui-même, il convient de rester prudent et de prêter attention au sort que la juridiction administrative réservera aux premiers recours introduits contre les délibérations du Comité de sécurité de l'information.

109 Articles 46, § 2, et 35/1, § 4, des lois du 15 janvier 1990 et du 15 août 2012.

110 Conformément à l'article 51 du règlement de la Chambre des représentants, l'urgence a été demandée par le Gouvernement au moment du dépôt du projet de loi et a été adoptée le 28 juin 2018.

111 Article 1er, § 3, du RGPD.