COMITÉ PERMANENT DE CONTROLE DES SERVICES DE RENSEIGNEMENT ET DE SÉCURITÉ

Numéro de notice 2020. 279

Enquête de contrôle sur la manière dont les services de renseignement belges communiquent avec un employeur, privé ou public, sur un collaborateur

7 avril 2021

I. INTRODUCTION 3
I.1. CONTEXTE ET OBJET DE L'ENQUÊTE 3
I.2. COMPÉTENCE DU COMITÉ PERMANENT R 3
II. LE CADRE GÉNÉRAL 3
III. L'EMPLOYEUR SOUHAITE UN SCREENING DE SÉCURITÉ 5
III.1. LA BASE LÉGALE POUR LES SCREENINGS DE SÉCURITÉ 5
III.2. ARTICLE 19, ALINÉA 1ER, PREMIÈRE PARTIE DE PHRASE L.R&S 6
IV. L'EMPLOYEUR FAIT L'OBJET D'UNE MENACE (PRÉSUMÉE) 6
IV.1. ARTICLE 19, ALINÉA 1ER, DERNIÈRE PARTIE DE PHRASE L.R&S 6
IV.2. DEUX ENQUÊTES DE CONTRÔLE ANTÉRIEURES DU COMITÉ 7
IV.3. UNE ÉLABORATION PLUS POUSSÉE DE CETTE RÉGLEMENTATION DANS UNE DIRECTIVE ? ... 8
IV.4. LES LIMITES POSÉES PAR LA LOI ORGANIQUE DES SERVICES DE RENSEIGNEMENT ET DE SÉCURITÉ (L.R&S) 9
IV.5. QU'EST CE QUI PEUT OU DOIT ÊTRE COMMUNIQUÉ ? 11
IV.5.1. LES PRINCIPES DE PROPORTIONNALITÉ ET DE SUBSIDIARITÉ 11
IV.5.2. LE PRINCIPE DE PRÉCAUTION 13
IV.5.3. DONNÉES CLASSIFIÉES 13
IV.5.4. COMMUNICATION ORALE OU ÉCRITE DES INFORMATIONS 13
V. CONCLUSIONS ET RECOMMANDATIONS 14

I. INTRODUCTION

I.1. CONTEXTE ET OBJET DE L'ENQUÊTE

En août 2019, le Comité permanent R a reçu une plainte d'une personne qui travaillait pour une institution publique. L'intéressé se plaignait que son employeur avait demandé des informations le concernant à un service de renseignement, et sur cette base, entendait entreprendre des démarches disciplinaires.

Au cours du traitement de la plainte, le Comité a décidé de commencer par effectuer une analyse juridique de la question plus générale des cas et des conditions dans lesquels une instance privée ou publique peut adresser une demande à l'un des deux services de renseignement sur un collaborateur (ou un candidat à un emploi) et, plus important encore, les cas dans lesquels le service de renseignement concerné peut ou doit y répondre et, le cas échéant, à quelles exigences cette réponse doit satisfaire.

I.2. COMPÉTENCE DU COMITÉ PERMANENT R

L'article 33 de la Loi du 18 juillet 1991 organique du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace (L.Contrôle) stipule que le Comité permanent R enquête sur les activités et les méthodes des services de renseignement et sur la manière dont ils remplissent leurs missions (légalité, efficience, efficacité). Les questions soulevées dans la présente enquête concernent exclusivement la légalité des actions d'un service de renseignement.

Le 16 décembre 2019, le Comité a sollicité un avis juridique externe. Il porte sur le respect du droit à la vie privée des travailleurs dans le cadre d'échanges éventuels entre des employeurs et les services de renseignement. L'avis juridique a été adressé au Comité permanent R le 14 avril 2020.

Le présent rapport reprend les conclusions des experts, combinées à l'analyse du Comité. Les citations reprises au fil du texte proviennent des avis des experts.

Dans son courrier du 26 février 2021, le SGRS a formulé quelques remarques sur cette enquête de contrôle. Ces remarques ont été intégrées là où c'était nécessaire dans le présent rapport.

Dans son e-mail du 29 mars 2021, la VSSE a fait savoir qu'elle n'avait aucune remarque sur le texte. Le service a néanmoins annoncé travailler sur une directive interne relative à la problématique concernée.

II. LE CADRE GÉNÉRAL

Qu'un service de renseignement fournisse des informations sur un collaborateur (ou un candidat à un emploi) d'initiative ou à la demande d'un employeur constitue dans les deux cas une ingérence dans la vie privée et dans le droit à la protection des données à caractère personnel, et ce même s'il s'agit d'une relation de travail. Une telle ingérence n'est permise que s'il existe une base légale claire, si l'ingérence poursuit un objectif légitime et si elle est proportionnée (article 8 CEDH, Convention 108 et 108+ et article 22 de la Constitution).

Dans ce cadre, il convient également de mentionner l'article 2 § 1er, alinéa 2, de la Loi du 30 novembre 1998 organique des services de renseignement et de sécurité (L.R&S), qui dispose que les services de renseignement *'[d]ans l'exercice de leurs missions (…) veillent au respect et contribuent à la protection des droits et libertés individuels, ainsi qu'au développement démocratique de la société'.*

Les experts, qui ont été désignés par le Comité, se sont exprimés en ces termes :

> *«* Un employeur (du service public) peut-il interroger un des services de renseignement belges aux fins de savoir si un de ses travailleurs (agents) est connu de ces services ?
>
> *1. Cette première question met au centre* ***l'employeur et la relation de travail*** *entre l'agent et l'employeur. Selon que l'employeur relève du secteur privé ou du secteur public, selon les législations et réglementations spécifiquement applicables à tel ou tel secteur, à tel ou tel employeur, des nuances peuvent infléchir la portée des restrictions ou ingérences autorisées.*
>
> *Dans tous les cas cependant, l'employeur devra justifier, s'il sollicite des informations à propos d'un agent et le contrôle à son insu, que son initiative est prévue par la loi, poursuit un but légitime et est proportionnée.*
>
> *En droit belge et dans le droit européen des droits humains, la seule qualité d'employeur invoqué sans autre justification légitime ne permet pas de rencontrer ces trois exigences. La relation de travail implique le respect au droit à la vie privée et non des restrictions ou ingérences dans celui-ci.*
>
> *Il en résulte que l'appréciation de la conformité au droit positif du comportement d'un tel employeur relève avant tout du contentieux de la relation de travail, dès lors que l'agent en est averti ou en prend connaissance, et des remédiations ou sanctions propres à ce contentieux. »*
>
> *« 2. On peut toutefois en inférer qu'****un service de renseignement*** *à qui une telle question serait adressée et qui envisagerait d'y répondre* ***veillera à ce que sa saisine soit régulière****, c'est-à-dire fondée sur une compétence légale pertinente, poursuivant un but légitime et enclose dans le principe de proportionnalité.*[1] *»*
>
> *« 3. Certes l'agent public voit sa position caractérisée par un* ***devoir de réserve et de dignité*** *et ceci peut commander des restrictions plus larges que pour les travailleurs ordinaires. Il n'en reste pas moins que la possibilité d'exercer un contrôle secret portant sur la vie privée d'un agent répond aux principes rappelés ci-dessus et détaillés comme suit dans la jurisprudence :*
>
> - *existence de dispositions légales habilitant à procéder à un contrôle secret à l'égard de l'intéressé ;*
> - *accessibilité et prévisibilité de ces dispositions, notamment la question de savoir si l'intéressé savait, au moment où il a été engagé, qu'il pouvait être exposé à un contrôle secret de ses activités ne relevant pas directement de sa mission ;*
> - *précision de ces dispositions (cas dans lequel un contrôle secret peut être pratiqué, type de mesures pouvant être pratiquées, conditions dans lesquelles ces mesures peuvent être opérées…) ;*
> - *étendue du contrôle pratiqué ;*
> - *garanties procédurales offertes par ces dispositions pour éviter tout arbitraire. »*

---

1 Dans ce cadre, le SGRS a affirmé ce qui suit : « *En principe, le SGRS demande la base légale qui fonde la demande de 'screening'. Néanmoins, il n'appartient pas au SGRS de vérifier que l'autorité qui pose la question respecte bien son cadre légal. C'est d'autant plus vrai lorsqu'elle transmet au SGRS des informations sur une menace potentielle. Le SGRS va traiter toute information pertinente qu'il reçoit, peu importe si l'autorité a, par exemple, violé son secret professionnel pour transmettre l'information. C'est la même chose pour une source ou un service partenaire. Il n'appartient pas au SGRS de 'contrôler' ses sources au sens large. Par contre il est évident qu'il ne transmettra des informations que si son cadre légal propre le lui permet.* »

Soyons clairs : aucune disposition de la L.R&S n'interdit qu'une instance privée ou publique adresse une demande à l'un des services de renseignement belges.

Si un employeur s'adresse à un service de renseignement, cela signifie inévitablement qu'il communique des données à caractère personnel à ce service, certainement s'il contextualise sa demande d'informations. Il s'agit ici aussi d'une ingérence dans la vie privée que seule une base légale claire rend possible. La L.R&S le permet dans la mesure où l'employeur croit raisonnablement que les informations peuvent être utiles pour l'exécution des missions du service de renseignement concerné (article 14 L.R&S concernant les acteurs publics ; article 16 L.R&S concernant les acteurs privés).

À la réponse apportée à la question de savoir si des informations provenant d'un service de renseignement peuvent être communiquées à un employeur privé ou public, il est également important d'attirer l'attention sur le secret professionnel spécifique et pénalement sanctionné auquel sont soumis les membres des services de renseignement (article 36 L.R&S). Cette disposition précise aussi que de tels flux d'informations ne sont possibles que si la loi le permet explicitement. Il convient de noter que la simple confirmation qu'une personne est ou n'est pas 'connue' d'un service de renseignement, sans entrer dans les détails, relève également de ce règlement.

Le législateur belge n'a prévu que deux cas dans lesquels un employeur (à son initiative ou à l'initiative du service de renseignement) peut obtenir directement ou indirectement des informations sur un collaborateur (ou un candidat à un emploi) : en cas de screening de sécurité ou en cas de menace. Même la simple question de savoir si un collaborateur (ou un candidat à un emploi)[2] est 'connu' ou non d'un des deux services de renseignement belges, doit pouvoir être associée à l'une de ces deux réglementations.

III. L'EMPLOYEUR SOUHAITE UN SCREENING DE SÉCURITÉ

III.1. LA BASE LÉGALE POUR LES SCREENINGS DE SÉCURITÉ

Les screenings de sécurité font référence aux situations dans lesquelles un employeur, indépendamment d'un élément antérieur, souhaite que toutes les personnes qui ont besoin d'une autorisation ou d'un permis donné(e) soient soumises à un screening. Les exemples les plus classiques sont ceux d'une habilitation de sécurité en vue d'avoir accès à des informations classifiées, l'attestation de sécurité pour un accès à un lieu ou à un événement déterminé, ou encore un avis de sécurité qui peut être demandé pour des dizaines d'autorisations différentes. Un employeur privé ou public peut recourir à ces options dans les conditions prévues par la Loi du 11 décembre 1998 relative à la classification, aux habilitations, attestations et avis de sécurité (Loi Classification) et par ses différents décrets d'application. De manière générale, le recours à ces instruments n'est autorisé que si l'utilisation abusive d'une autorisation ou d'un permis (par ex. par un collaborateur) est susceptible de nuire aux intérêts fondamentaux de l'État.

En principe, l'employeur ne sera pas informé des données à caractère personnel qui résultent de la vérification ou de l'enquête. Il ne recevra généralement que le résultat du screening : l'habilitation ou l'attestation de sécurité est ou n'est pas octroyée ; l'avis de

[2] Par souci de clarté, il convient de souligner que l'analyse ci-dessous s'applique intégralement à tout statut « protégé » qui s'appliquerait à un collaborateur.

sécurité est positif ou négatif. C'est l'officier de sécurité[3] qui sera informé des éléments concrets du dossier. Mais cet officier de sécurité sera soumis à son tour à un secret professionnel spécifique et sanctionné pénalement (articles 23 et 24 de la Loi Classification). Il ne peut pas communiquer sans autre forme de procès à l'employeur les éléments dont il dispose.

La Loi Classification ne prévoit pas uniquement un screening et la communication des informations dans le cadre de l'autorisation ou du permis initial. Dans certains cas (par ex. une habilitation de sécurité), le collaborateur est soumis à une forme de 'screening permanent'. En d'autres termes, pendant toute la durée de son habilitation, il devra répondre aux exigences pour disposer de cette habilitation. Si, à un moment donné, un employeur doute de cette condition, il peut consulter son officier de sécurité, qui peut à son tour saisir l'autorité de sécurité et/ou le service de renseignement ayant effectué l'enquête. Mais rien n'empêche l'employeur de prendre contact directement avec un service de renseignement s'il estime disposer d'informations utiles pour l'exercice de ses missions (articles 14 ou 16 L.R&S).

En ce qui concerne les screenings de sécurité, il importe donc de souligner que la réglementation légale détermine clairement quelles données à caractère personnel (par ex. les données énumérées à l'article 22*sexies* de la Loi Classification et dans l'A.R. du 8 mai 2018 pris en exécution de cette disposition) peuvent être transmises, sous quelle forme (par ex. un rapport d'enquête) et à quel destinataire (généralement une autorité de sécurité).

III.2. ARTICLE 19, ALINÉA 1ER, PREMIÈRE PARTIE DE PHRASE L.R&S[4]

Enfin, le Comité réaffirme que l'article 19 L.R&S ne constitue pas une base pour la transmission systématique d'informations aux employeurs qui en font la demande dans le cadre des autorisations ou des permis qu'ils doivent accorder.[5]

IV. L'EMPLOYEUR FAIT L'OBJET D'UNE MENACE (PRÉSUMÉE)

IV.1. ARTICLE 19, ALINÉA 1ER, DERNIÈRE PARTIE DE PHRASE L.R&S

L'article 19 L.R&S s'énonce comme suit : *'Les services de renseignement et de sécurité ne communiquent les renseignements visés à l'article 13, deuxième alinéa (…) qu'aux instances et personnes qui font l'objet d'une [menace] visée aux articles 7 et 11.'*

---

3 L'officier de sécurité est la personne désignée au sein d'une instance privée ou publique qui est chargée de faire respecter les règles en matière de classification. Il est également la personne de contact entre l'instance, l'intéressé et l'autorité de sécurité compétente.

4 Le premier paragraphe complet de l'article 19 L.R&S se lit comme suit : *'Les services de renseignement et de sécurité ne communiquent les renseignements visés à l'article 13, deuxième alinéa, qu'aux ministres et autorités administratives et judiciaires concernés, aux services de police et à toutes les instances et personnes compétentes conformément aux finalités de leurs missions ainsi qu'aux instances et personnes qui font l'objet d'une [menace] visée aux articles 7 et 11.'*

5 L'enquête a montré que le Service Vérifications de Sécurité de la VSSE réalise des screenings sans indication claire de la base légale (*supra*). Dans certains cas, la finalité de la demande n'est pas précisée : s'agit-il d'un screening de sécurité ou d'un contrôle dans la banque de données de la VSSE ? À cet égard, la VSSE se référait systématiquement (à tort, *supra*) à l'article 19 L.R&S. S'il peut être utile et conseillé de consulter les services belges à propos des résidents belges pour lesquels un accès à des installations d'instances internationales établies en Belgique devrait éventuellement être autorisé, un mandat légal est requis à cet effet (COMITÉ PERMANENT R, *Rapport d'activités 2019*, 2 et suiv.).

Cette disposition constitue une base légale claire pour un service de renseignement aux fins de communication de données (à caractère personnel) à des personnes ou à des instances publiques ou privées[6], et donc, le cas échéant, également à un employeur dont le collaborateur représente une des menaces que doit suivre la VSSE ou du SGRS en vertu de la loi.

Cette disposition constitue aussi, en combinaison avec l'article 14 ou 16 L.R&S, la base légale pour un employeur public ou privé inquiet qui interroge un service de renseignement sur son collaborateur parce qu'il estime qu'il représente une menace (potentielle) au sens de la L.R&S. Ces dispositions constituent également la base juridique permettant de communiquer, en réponse à cette question, des éléments concrets sur le collaborateur qui peuvent rendre la menace (présumée) plausible.[7]

Cette communication/question peut naturellement donner lieu, pour un service de renseignement, à l'ouverture d'une enquête de renseignement. D'un point de vue juridique, l'ouverture ou non d'une telle enquête, plus ou moins approfondie, est distincte de la question de savoir si et ce qu'un service de renseignement peut communiquer à un employeur.[8]

IV.2. DEUX ENQUÊTES DE CONTRÔLE ANTÉRIEURES DU COMITÉ

En 2014-2015, le Comité a effectué une enquête qui faisait suite à une plainte. L'application de la dernière partie de la phrase de l'article 19, alinéa 1er L.R&S y occupait une place centrale.[9] Un condensé des résultats est repris ci-dessous. Différents aspects de ce résumé seront approfondis par la suite.

Selon le plaignant, le contenu d'e-mails personnels qu'il avait envoyés à un membre du ministère de la Défense aurait atterri chez son employeur via le service de renseignement militaire. Peu après, son employeur lui a signifié son licenciement, en se référant explicitement à la transmission par un collaborateur du SGRS d'une copie des e-mails concernés. L'enquête devait établir de quelle manière le SGRS avait traité le dossier, si le service avait respecté la réglementation en vigueur, et si des informations avaient en effet été transmises à un tiers. Les e-mails en question étaient arrivés au SGRS par l'intermédiaire d'un membre du ministère de la Défense. Dans ses messages, le plaignant avait effectivement mentionné – en guise de plaisanterie, comme avéré par la suite – qu'il avait transmis un virus informatique. Le SGRS

---

6 La loi ne fait référence qu'à des 'instances et personnes'. La loi fait uniquement référence aux 'instances et personnes'. Il n'y a aucune raison de croire que cette réglementation, hormis la première partie de phrase de l'article 19, alinéa 1er L.R&S, serait limité aux personnes (morales) publiques.

7 Aucune disposition de la L.R&S n'interdit à un employeur de poser des questions à un service de renseignement. Au contraire, si un service public estime que des informations sensibles sont menacées d'être compromises ou que des menaces d'espionnage ou d'ingérence dans les processus décisionnels peuvent exister, rien n'interdit aux responsables de ce service public de s'adresser au service de renseignement le plus compétent. Rien n'empêche par conséquent un employeur d'un service public de communiquer des informations ou de poser des questions concernant l'un des membres de son personnel. Cela ne signifie cependant pas que les services de renseignement peuvent ou doivent répondre à la question posée. Le fait que le service de renseignement ne peut (ou ne veut pas) répondre à une question ne rend pas illégal ou fautif le fait d'avoir posé la question.

8 Il n'est évidemment pas légitime d'initier une enquête (par définition attentatoire à la vie privée) en l'absence de tout élément indiquant une menace potentielle ou concrète contre les intérêts fondamentaux de l'État.

9 COMITÉ PERMANENT R, *Rapport d'activités 2015*, 41 et suiv. ('II.9. Plainte relative à la transmission d'informations à caractère personnel à un tiers par un agent de renseignement').

est le service approprié pour examiner ce genre de menace potentielle, cette tâche relevant de ses missions légales. Outre cette enquête de nature informatique, le recueil de renseignements du SGRS sur le plaignant lui-même a également été effectué dans le cadre de ses compétences, puisqu'il s'agissait d'évaluer la menace éventuelle. Cela fait aussi partie de ses compétences. Le résultat de cette enquête technique (qui a démontré l'absence de menace) a été communiqué en termes généraux à l'officier de sécurité de l'entreprise où le plaignant était employé. Comme le Comité l'a estimé à l'époque, cette communication trouvait son fondement légal dans l'article 19 L.R&S.

Dans une autre enquête de contrôle[10] également, le Comité permanent R s'était exprimé sur l'applicabilité de cette disposition. Le Comité s'interrogeait sur les 'contre-mesures' qui pouvaient être prises si des services de renseignement étrangers recueillaient secrètement des renseignements à propos leur diaspora sur le territoire belge : '*Il est de toute façon clair qu'ils ne peuvent pas intervenir « activement » pour influencer le cours des événements. Le cadre légal ne prévoit que des possibilités restreintes d'intervention directe. En pratique, le responsable de la VSSE ou du SGRS ne peut qu'interpeller oralement son collègue étranger ou informer la diaspora des activités qu'un service de renseignement étranger entreprend à l'égard de cette communauté*', et ce sur base de la partie de phrase concernée de l'article 19 L.R&S.

IV.3. UNE ÉLABORATION PLUS POUSSÉE DE CETTE RÉGLEMENTATION DANS UNE DIRECTIVE ?

Le Comité considère certes que la dernière partie de phrase de l'article 19, alinéa 1er L.R&S est une base juridique suffisamment claire pour la communication d'informations à des instances publiques et privées[11], mais il existe une obligation d'en préciser les modalités.

Conformément à l'article 20 § 3 L.R&S, le Conseil national de sécurité doit définir, dans une directive, les conditions dans lesquelles des renseignements peuvent être communiqués à des instances ou à des personnes privées ou publiques. Pour autant que le Comité ait pu le constater, cette obligation n'a, jusqu'à présent, pas été remplie en ce qui concerne la situation des personnes et des instances qui font l'objet d'une menace. Dans le cadre d'une enquête portant sur la lutte contre le terrorisme et l'extrémisme, le Comité avait déjà insisté sur la nécessité d'une telle directive.[12] Il réitère sa recommandation avec force. La directive doit

---

10 COMITÉ PERMANENT R, *Rapport d'activités 2012*, 14 et suiv. ('II.2. Le suivi par certains services de renseignement étrangers de leur diaspora en Belgique').

11 Concernant la possibilité prévue à l'article 19, alinéa 1er L.R&S de communiquer des informations aux autorités judiciaires, le Comité s'est interrogé sur la qualité de cette réglementation : '*Cette disposition répond-elle au principe de prévisibilité [comme visé à l'article 8 CEDH et à l'article 22 de la Constitution, ndr] ? Un citoyen sait-il que les données collectées par un service de renseignement à son sujet dans un but A peuvent être transmises à une autre autorité dans un but B ? Et ce but B, a-t-il toujours une finalité légitime au sens de l'article 8 CEDH ? Qu'en est-il de la proportionnalité ? Ces questions se posent moins pour la communication d'informations à la Justice. Le Comité Permanent R est néanmoins d'avis que l'application de l'article 19 devrait être développée plus avant dans une directive publique à prendre par le Comité Ministériel du Renseignement et la Sécurité en exécution de l'article 20.* ' (COMITÉ PERMANENT R, *Rapport d'activités 2004*, 120).

12 *'Les services de renseignement doivent élaborer des critères pour informer les personnes qui font l'objet d'une menace (article. 19 L.R&S).'* Le Comité recommandait que les deux services de renseignement élaborent des critères en vue de l'application de cette disposition (COMITÉ PERMANENT R, *Rapport d'activités 2012*, 92).

offrir des points d'appui aux services de renseignement dans cette matière délicate, où la communication ou la non-communication des informations peut avoir de graves répercussions sur l'intérêt général et sur les intérêts privés.

Aucune autre réglementation n'a été élaborée à cet égard au niveau des services de renseignement non plus.

Le SGRS a déclaré ne pas disposer de directive interne/SOP décrivant la manière dont son personnel doit traiter cette problématique.[13]

En ce qui concerne la VSSE, il peut être fait référence à deux directives. Il y a tout d'abord l'instruction du 10 octobre 2016 classifiée 'CONFIDENTIEL' qui traite de la manière dont le service doit réagir en cas de demande d'une autorité publique de procéder à des vérifications concernant une personne déterminée. Cette directive ne précise pas sur la base de quelle législation certaines réponses doivent être apportées. La directive ne semble pas s'appliquer à la situation prévue dans la dernière partie de phrase de l'article 19, alinéa 1er L.R&S. En tout cas, elle ne règle pas les relations avec les acteurs privés. Le Comité s'interroge du reste sur la légalité de certains passages de cette directive, car ceux-ci vont apparemment à l'encontre de la réglementation sur les screenings de sécurité. Ensuite, la VSSE a établi en 2018 une directive classifiée 'CONFIDENTIEL' sur les actions disruptives ou les entraves. Il s'agit d'entraver les menaces à un point tel qu'elles ne se produisent plus ou que leur nuisibilité s'en trouve considérablement réduite. Si la communication d'informations à une personne ou à une instance faisant l'objet d'une menace peut parfaitement entrer dans cette définition, aucune référence n'est faite dans cette directive à l'article 19 L.R&S, ni à aucune autre disposition légale.

Le Comité demande donc instamment au Conseil national de sécurité d'émettre une directive générale et complète. Cette directive doit en tout cas apporter une réponse aux questions et points d'attention ci-dessous.

IV.4. LES LIMITES POSÉES PAR LA LOI ORGANIQUE DES SERVICES DE RENSEIGNEMENT ET DE SÉCURITÉ (L.R&S)

Dans quels cas et dans quelles limites un service de renseignement peut-il actuellement faire usage de la possibilité d'informer un tiers (public ou privé) des informations dont il dispose ?

En ce qui concerne la VSSE, les menaces visées à l'article 19 L.R&S sont toutes les activités d'espionnage, d'ingérence, de terrorisme, d'extrémisme, de prolifération, ainsi que toutes activités menées par des organisations sectaires nuisibles ou des organisations criminelles susceptibles de mettre en péril la sûreté intérieure de l'État et la pérennité de l'ordre démocratique et constitutionnel, la sûreté extérieure de l'État, la sauvegarde du potentiel scientifique ou économique, tel que défini par le Conseil national de sécurité, ou tout autre intérêt fondamental du pays (article 7 L.R&S). Il doit non seulement y avoir une activité bien définie dans le chef du collaborateur (par ex. l'extrémisme), mais celle-ci doit également représenter un danger pour un ou plusieurs intérêts fondamentaux de l'État. Dans le contexte de l'article 19 L.R&S, cette instance privée ou publique doit, en outre, faire l'objet d'une

[13] Le SGRS souligne le fait que, dans ce cadre, il se base sur les réglementations légales existantes (la Loi du 11 décembre 1998 relative à la classification, pour les vérifications ; l'article 19 de la Loi organique des services de renseignement et de sécurité, pour la communication des informations aux employeurs en cas de menace ; d'autres dispositions légales).

menace. Un employeur ne peut donc pas être informé, par exemple des activités extrémistes de son collaborateur, s'il (lisez : l'employeur) ne fait nullement l'objet d'une menace.

Il est tout aussi clair que l'article 19 L.R&S ne peut être appliqué lorsque les intérêts fondamentaux de l'État ne sont aucunement en jeu, comme par exemple porter atteinte à l'image d'une entreprise privée (sauf si cela signifie, par exemple, une perte de confiance dans certaines instances), une mauvaise ambiance de travail ou une perte financière (sauf si ces intérêts financiers dépassent les intérêts individuels de l'entreprise et peuvent être considérés comme fondamentaux pour le pays).

Les menaces qui peuvent amener le SGRS à avertir des instances ou personnes privées ou publiques figurent à l'article 11 L.R&S. Il s'agit, par exemple, de toute activité qui représente une menace pour l'intégrité du territoire national ou la population, les plans de défense militaires, le potentiel scientifique et économique dans les secteurs économiques et industriels liés à la défense, l'accomplissement des missions des Forces armées, la sécurité militaire du personnel relevant du Ministre de la Défense nationale.

Étant donné que la communication de données sur la base de la dernière partie de phrase de l'article 19, alinéa 1er L.R&S a une finalité clairement définie (sauvegarde des intérêts fondamentaux de l'État contre certaines activités dont l'instance ou la personne concernée fait l'objet), cette communication doit également se limiter aux informations qui contribuent au suivi ou, si nécessaire, à la neutralisation de la menace.

> *« Avant de répondre et en vue de répondre, les services de renseignement s'assureront en conséquence du fondement, de la motivation et de la pertinence de la question relative à un agent qui leur est adressée. Nul doute que s'ils réservent une réponse aux questions qui leur sont posées (ceci relève davantage de la deuxième question ci-après), ils engagent leur responsabilité. Nous visons bien ici le fait* ***de répondre*** *aux questions posées par un employeur, et non le fait de diligenter une enquête pour les besoins propres des services, à la suite des questions posées, sans répondre à ces dernières. »*
>
> *« 4. Tout employeur normalement prudent et diligent veillera donc à cadrer sa demande dans le respect de ces principes. Il sera prudent, pour les services, de veiller à ne répondre le cas échéant qu'à des demandes satisfaisant à ces exigences. À défaut, la communication des informations par les services pourrait constituer une violation du droit à la protection de la vie privée dans les organes juridictionnels et non juridictionnels de contrôle pourront être saisis : c'est tout l'objet de la deuxième question. »*
>
> *« La question est de savoir si le service de renseignement est tenu de répondre, s'il peut répondre ou si, au contraire, il lui est interdit de répondre.*
>
> *5. La réponse à cette question doit être analysée au regard des* ***missions assignées au service de renseignement*** *: le principe de finalité commande la réponse. Le service doit n'avoir en vue que l'accomplissement de sa mission propre ; il ne peut accepter d'être instrumentalisé. En d'autres termes, il n'a aucune obligation de répondre, voire même il lui est interdit de répondre sauf dans la mesure où la bonne fin des missions propres qui lui sont confiées commande de répondre.*
>
> *L'éventuelle obligation de répondre ne peut venir que d'une* ***législation spécifique*** *conférant au service de renseignement* ***une mission*** *dont découle cette obligation, et non de la demande qui lui est adressée par un employeur. Une telle obligation éventuelle aura toujours le statut d'une exception à la règle : le respect au droit de la vie privée des agents. »*

La première obligation d'un service de renseignement qui se voit confronté à une demande d'informations est par conséquent de vérifier de quel problème, de quel incident, de quelle menace il pourrait s'agir. Dans ce cadre, le service de renseignement pourrait interroger ses

banques de données pour vérifier le (ou les) nom(s) qui lui est (sont) communiqué(s).[14] Il apparaît aussi évident que le service de renseignement prenne contact avec l'employeur afin de bien contextualiser la demande. À cet effet, il conviendra de déterminer notamment pourquoi l'employeur veut savoir si son collaborateur est connu des services de renseignement, quel est le problème et la menace, s'il y a eu un incident de sécurité ou autre, une urgence, etc.

Si ces données ne sont pas concluantes dans un sens ou dans l'autre, une enquête plus approfondie du service peut être indiquée. L'amplitude de cette enquête ne peut être déterminée *in abstracto*. Elle dépendra de la nature de la menace et des informations qui apparaîtront au cours de l'enquête. Dans le cadre d'une telle enquête, le service devra en tout cas tenir compte des principes de proportionnalité et de subsidiarité.

Les réponses à ces questions et les résultats de l'enquête complémentaire doivent permettre au service de renseignement d'évaluer s'il est compétent en la matière et, le cas échéant, s'il peut appliquer l'article 19 L.R&S. Ces réponses doivent également permettre au service de renseignement de déterminer ce qu'il peut ou non communiquer à l'employeur compte tenu de la menace.

IV.5. QU'EST CE QUI PEUT OU DOIT ÊTRE COMMUNIQUÉ ?

Tout d'abord, l'hypothèse brièvement évoquée est celle du service de renseignement qui n'identifie *absolument aucune* menace dans le chef du collaborateur au sens de la L.R&S (éventuellement après avoir questionné une première fois ledit collaborateur ou après une enquête plus approfondie). À ce moment-là, l'employeur ne fait, par définition, pas l'objet d'une menace et *sensu stricto* l'article 19 L.R&S ne peut être appliqué. Le Comité estime cependant que dans ces cas, le service de renseignement doit avoir la possibilité d'informer l'employeur qu'il n'y a pas de menace au sens de la L.R&S (ce qui ne signifie évidemment pas que l'employeur ne peut pas faire l'objet d'une autre menace). Le Comité s'est déjà prononcé en ce sens dans l'enquête menée en 2014-2015 qui faisait suite à une plainte (voir IV.2.).

Dans ce qui suit, on part du principe qu'il existe effectivement une menace. La question se pose alors de ce qui peut être communiqué de quelle manière.

IV.5.1. Les principes de proportionnalité et de subsidiarité

> *« 6. Les limites de la réponse éventuelle sont circonscrites* ***par la loi du 30 novembre 1998 organique des services de renseignement et de sécurité, qui doit être mise en œuvre en combinaison avec l'article 74 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.***
>
> *On voit que le traitement des données impliquant la communication de celle-ci à l'employeur est licite :*
> – *lorsqu'il est "utile" au respect des obligations incombant au service de renseignement ;*
> – *ou lorsqu'il est "nécessaire" (et non seulement "utile" ; on retrouve ici le principe de nécessité qui est au cœur du principe de proportionnalité) à la mission dont est investie de l'autorité publique destinataire des informations communiquées par le service de renseignement. »*
>
> *« 7. On mesure donc les limites très strictes dans lesquelles doit être contenue une réponse éventuelle du service de renseignement. Pour que le service puisse répondre, il faut qu'il ait à transmettre des*

[14] C'est également ce que prescrit la directive de la VSSE du 10 octobre 2016 ('CONFIDENTIEL') dans le cadre d'une demande adressée par une autorité publique en vue de faire procéder à des vérifications sur une personne.

*informations résultant du traitement de données à caractère personnel qui soit **« nécessaire » à la mission dont est investie l'autorité publique destinataire** des informations communiquées.*
*En d'autres termes, s'il est toujours licite que le service de renseignement puisse procéder au traitement de données consistant en une collecte de données pertinentes et à jour lorsque celui-ci est simplement **« utile » à l'accomplissement de ses obligations propres**, ceci ne lui donne pas pour autant l'autorisation de communiquer ces informations et de répondre ainsi à la demande qui lui a été adressée. Elle ne le pourra que si le résultat du traitement se révèle nécessaire à la bonne fin de la mission de l'autorité qui l'aura interrogée. »*

*« 8. Pour rappel, **ce rapport de nécessité s'interprète restrictivement** dès lors que l'on est dans le domaine des ingérences et restrictions aux droits au respect de la vie privée.*
La seule existence d'un lien d'emploi non autrement qualifié n'est pas de nature à justifier cette nécessité. Il faudrait encore que l'autorité ayant interrogé la sûreté ait été en mesure de décrire et de justifier les faits spécifiques pertinents (responsabilité spécifique de l'agent, dimension opérationnelle propre de son emploi…) qui justifieraient la communication des données « nécessaires » pour la bonne fin de la mission propre de cette autorité.

– *À défaut, la demande comme l'éventuelle réponse que cette demande aura appelée constitueront une violation du droit à la protection de la vie privée dont les organes juridictionnels ou non juridictionnels de contrôle pourront être saisis. »*

Compte tenu des exigences de proportionnalité et de subsidiarité, la première question doit être de savoir si l'employeur doit absolument être informé. Si la menace est très vague et peu grave, ou si le service peut lui-même suivre l'évaluation de la menace ou encore si la menace peut être contrée d'une autre manière (par ex. en s'adressant au collaborateur de sorte qu'il soit conscient d'être suivi), il se peut que la communication de données à caractère personnel à un employeur soit disproportionnée et non subsidiaire.

Si cela ne suffit pas et que la menace est suffisamment grave, la possibilité se présente alors d'en informer l'employeur. Ici aussi, il faut tenir compte de la quantité et du type d'informations qui sont données. Une fois encore, la règle est que, compte tenu de la nature et de la gravité de la menace et de la nécessité et des options disponibles pour les contrer, l'objectif doit être une ingérence minimale dans la vie privée.

Cependant, si la menace est si grave qu'elle ne peut être contrée que par l'intervention de l'employeur, davantage d'informations et des informations plus concrètes peuvent être communiquées. Ces informations peuvent, par exemple, servir à motiver une décision administrative ou privée (une sanction disciplinaire, une mutation, un licenciement, etc.). De toute évidence, l'objectif ultime du service de renseignement doit être dans ce cas-ci de neutraliser ou d'atténuer une menace.

Dans le prolongement de la question de la communication proportionnée des informations, un service de renseignement peut-il, dans le cadre de sa communication, lui-même proposer une solution à l'instance publique ou privée[15] qui est menacée, voire participer à la prise de décision de l'instance ou de la personne menacée sur la manière de traiter cette menace (par ex. suggérer un licenciement) ? Le Comité estime que ceci n'est pas illégal dans la mesure où la solution qui est suggérée est elle-même légale et proportionnée.

Enfin, la question se pose de savoir si l'article 19 L.R&S prévoit une *obligation* de répondre à une question ou de fournir des informations *d'initiative*. La disposition prévoit que les services de renseignement et de sécurité *'ne communiquent'* leurs renseignements *'qu'aux'* instances et personnes qui font l'objet d'une menace. Même si la disposition dans ce domaine n'est pas très claire, le Comité estime qu'un service de renseignement est tenu de

[15] C'est ce que la VSSE appelle une 'entrave secondaire'.

communiquer des données s'il s'agit du seul moyen d'empêcher la concrétisation d'une menace grave contre les intérêts fondamentaux de l'État. Dans les autres cas, le service définit la meilleure stratégie en toute autonomie, en fonction de la menace.[16] Le Comité recommande de pallier ce manque de clarté, soit via une initiative législative, soit via un règlement en la matière dans la directive que doit émettre le Conseil national de sécurité.

Dans la foulée, le Comité suggère d'examiner s'il serait utile de prévoir une notification obligatoire à l'employeur pour chaque collaborateur (ou candidat à un emploi) figurant dans une Banque de données commune Terrorist Fighters ou Prédicateurs de haine.

IV.5.2. Le principe de précaution

Dans le cadre de tout ce qui précède, il convient également de prêter attention à la qualité de la communication des données. Dans un contexte de renseignement, il y a peu de certitudes, et ce fait doit influencer la décision d'informer ou non un employeur ainsi que la manière de le faire. Pour pouvoir être considérée comme légale, la communication d'informations doit être suffisamment étayée par des informations fiables. Elle doit également être formulée avec précaution. Par exemple, aucune image sans nuance ne peut être donnée des renseignements sous-jacents, ou un élément particulier ne peut être présenté comme étant une 'vision de' ou une 'impression de'. En ce sens, les informations fournies doivent également être 'justes' en offrant une image objective de la façon dont le service de renseignement perçoit la menace et le rôle de la personne concernée, sans être 'manipulatrices' au sens où elles viseraient à orienter les décisions des employeurs privés ou publics.

IV.5.3. Données classifiées

Toutes les instances privées et publiques ne disposent pas d'une habilitation de sécurité, ce qui signifie que les informations classifiées devront être déclassifiées. Ceci est d'autant plus vrai si les informations doivent servir à étayer une décision de l'employeur. Naturellement, cette opération doit également être réalisée avec soin. D'une part, ce qui doit rester secret doit rester secret ; d'autre part, les informations doivent permettre à l'employeur (et éventuellement plus tard au collaborateur et même à une juridiction) d'apprécier la valeur de l'information.

IV.5.4. Communication orale ou écrite des informations

L'article 19 L.R&S ne précise pas comment informer une autorité qui est menacée. Le Comité estime que, pour des raisons de sécurité juridique, cette notification devrait se faire par écrit,

---

16 Également en ce qui concerne la communication d'informations aux autorités judiciaires (première partie de phrase de l'article 19, alinéa 1er L.R&S), le Comité s'était précédemment exprimé en ces termes : '*Sa rédaction ambiguë ne nous permet pas d'y trouver une réelle obligation de transmettre des renseignements. Cette disposition est rédigée de telle sorte qu'elle implique plutôt une interdiction de communiquer certains renseignements à d'autres autorités que celles qu'elle cite. Cela signifierait la possibilité de communiquer d'autres informations. La directive que le Comité Ministériel du renseignement et de la sécurité devrait prendre en exécution de l'article 20, § 3 pourrait certes créer une obligation. Le Comité Permanent R n'a connaissance d'aucune directive de ce genre*.' (COMITÉ PERMANENT R, *Rapport d'activités 2004*, 119).

sauf en cas d'urgence. Il s'agit d'éviter les discussions après coup et de permettre un contrôle parlementaire, et même judiciaire.

Le Comité a déjà recommandé à cet égard que la VSSE clôture toute analyse par une conclusion (qu'elle soit sommaire ou provisoire) en vue d'établir si, comment et avec quelle intensité l'objet de l'analyse (personne, groupement, événement ou phénomène) doit continuer à être suivi.[17]

V. CONCLUSIONS ET RECOMMANDATIONS

Des règles strictes s'appliquent, à juste titre, à la communication d'informations par les services de renseignement à un employeur privé ou public. En effet, la communication d'informations peut avoir des conséquences non négligeables pour les personnes concernées. À tout le moins, cela signifie une atteinte à la vie privée et, dans les cas extrêmes, cela peut constituer la base de mesures intrusives pouvant affecter la situation juridique des intéressés.

Si la VSSE et la SGRS fournissent des informations à un employeur public ou privé, que ce soit d'initiative ou sur demande (en ce compris le fait de simplement informer que la personne est 'connue' ou non), ils doivent respecter toutes les exigences légales, à savoir :

1. L'existence d'une base légale spécifique ;
2. La vigilance est de rigueur au sein du service dans la production interne des données à fournir et dans leur communication au destinataire ;
3. La communication doit répondre aux exigences de nécessité ; et
4. La communication doit être proportionnée.

En ce qui concerne la base légale, le Comité souligne qu'en dehors des deux situations évoquées (c.-à-d. l'employeur veut un screening de sécurité ou le l'employeur fait l'objet d'une menace), il n'est pas permis de fournir des informations sur un collaborateur à un employeur public ou privé. Du point de vue de l'agent de renseignement, ce genre de communication peut même être punissable en fonction de la situation concrète.

Le Comité souligne également que rien n'empêche un employeur du secteur public ou privé de communiquer des informations ou d'interroger un service de renseignement belge concernant une éventuelle menace, au sens de la Loi du 30 novembre 1998 organique des services de renseignement et de sécurité (L.R&S), dont l'un des membres de son personnel serait l''auteur'.

Le Comité invite cependant les acteurs des secteurs publics et privés à examiner si certaines menaces potentielles ne peuvent pas être évitées en recourant, pour certaines fonctions, autorisations ou permis, au système de screening de sécurité prévu dans la Loi Classification. Le Comité insiste toutefois sur un recours judicieux, donc non débridé, à ce système.

Le Comité estime que la VSSE et le SGRS, dans les six mois suivant la conclusion de cette étude, doivent proposer une directive visant à mettre en œuvre la dernière partie de phrase de l'article 19, alinéa 1er L.R&S à l'attention des ministres de la Justice et de la Défense, en leur demandant de soumettre la proposition au Conseil national de sécurité pour approbation.

[17] COMITÉ PERMANENT R, *Rapport d'activités 2013*, 115.

La VSSE doit en outre évaluer les deux directives dont il était question ci-dessus et les adapter au cadre légal. Compte tenu de l'importance de cette matière, cette adaptation doit également avoir lieu dans un délai de six mois.

Par ailleurs, le Comité recommande au législateur de préciser si l'article 19, alinéa 1er, dernière phrase L.R&S contient également une *obligation,* dans certains cas, de répondre à une question ou de fournir des informations *de sa propre initiative*. Dans l'attente d'une initiative législative, cette question doit être réglée dans la directive du Conseil national de sécurité.

Dans la foulée, le Comité suggère d'examiner s'il serait utile de prévoir une notification obligatoire à l'employeur pour chaque collaborateur (ou candidat à un emploi) figurant dans une Banque de données commune Terrorist Fighters ou Prédicateurs de haine.