

crise, une réflexion de fond devrait maintenant se tenir en vue de baliser non seulement les conditions juridiques du déploiement de l'application éventuelle, mais égale-

ment les conditions d'utilisation qui permettraient d'en tirer un bénéfice réel. Pour mieux gérer la prochaine crise...

■ **Thierry Léonard**

Professeur à l'Université St Louis-Bruxelles
Avocat et DPO

Secteur public

Le traitement des données personnelles par la police et les autorités judiciaires dans le domaine pénal

La collecte et le traitement des données personnelles dans le domaine pénal ont récemment connu leur lot de réformes. Ce n'est toutefois pas le RGPD qui en est à l'origine¹, mais bien une directive européenne qui, adoptée à la même date que le règlement², a connu un retentissement nettement moins important.

Son contenu n'en est pourtant pas moins fondamental dès lors que la protection des personnes à l'égard du traitement de leurs données personnelles reste l'un des objectifs principaux de la directive³, qui couvre l'ensemble du domaine pénal, de la prévention et la détection des infractions jusqu'à l'exécution des peines, en passant par les enquêtes et les poursuites judiciaires. La directive s'astreint au difficile exercice d'assurer l'équilibre entre la protection des personnes et les finalités sécuritaires à l'occasion du traitement des données personnelles dans le domaine pénal. Cette approche, qui diffère de la perspective de construction du *marché unique (numérique)* du RGPD, justifiait l'adoption d'un cadre juridique distinct.

En Belgique, la directive a été transposée par la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel⁴ (soit la loi dans laquelle se trouvent également les règles d'exécution du RGPD⁵), à laquelle nous limiterons notre analyse dans la présente contribution. C'est précisément le titre II et, dans une moindre mesure, le titre VII⁶ de la loi qui ont assuré la transposition, en droit belge, de la norme européenne.

À l'instar du RGPD, le traitement des données personnelles dans le domaine pénal appelle de nombreux développements sur lesquels le format de notre analyse ne

nous permet pas de nous pencher. Plutôt que de prétendre à l'exhaustivité⁷, nous avons dès lors choisi de focaliser notre attention sur trois sujets : le champ d'application des dispositions applicables, de façon à distinguer celui-ci par rapport aux règles du RGPD ; le droit d'accès des individus aux données personnelles collectées et traitées dans le domaine pénal, tel qu'il est garanti par l'article 8, § 2, de la Charte des droits fondamentaux de l'Union européenne, ainsi que leur droit à l'information et à la rectification ; et les particularités de l'autorité de contrôle instituée dans ce domaine spécifique.

1. La protection des données personnelles dans le domaine pénal : quelques précisions en termes de champ d'application

Le traitement⁸ des données des personnes physiques reste l'élément central de la protection mise en place par la directive et la loi belge. C'est toutefois le domaine d'application de la réglementation qui les distingue du RGPD : il est, en effet, question du traitement de données « par les autorités compétentes » et « aux fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces »⁹.

a) Les finalités pénales

Les activités relevant des finalités pénales visées par la loi sont larges : elles recouvrent l'ensemble des activités policières (de nature judiciaire ou administrative), en ce compris les activités de maintien de l'ordre lors des manifestations, des grands événements sportifs ou des

¹ Le RGPD ne s'applique pas au traitement de données à caractère personnel effectué par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre des menaces pour la sécurité publique et la prévention de telles menaces. Voy. art. 2, § 2, d), 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, *J.O.U.E.*, n° L 119 du 4 mai 2016, p. 1 (ci-après « le RGPD »).

² Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, *J.O.U.E.*, n° L 119 du 4 mai 2016, p. 89 (ci-après « la directive »).

³ Assurer la libre circulation des données dans le cadre de l'Espace de liberté, sécurité et justice européen en est un autre. Ce second objectif ne fera toutefois pas l'objet de cette courte contribution.

⁴ M.B., 5 septembre 2018 (ci-après « la loi »). Soit tardivement par rapport à la date de transposition de la directive, fixée au 6 mai 2018. Art. 63, § 1^{er}, de la directive.

⁵ La loi contient en outre des dispositions relatives aux activités de traitement de données d'autorités qui sortent du champ d'application du droit de l'Union

européenne, telles que les forces armées, les services de renseignements et de sécurité, ainsi que dans le cadre de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité (titre III).

⁶ Le titre VII contient les dispositions applicables à l'Organe de contrôle de l'information policière, soit l'autorité de contrôle indépendante dont question à l'article 71 de la loi.

⁷ Pour plus de développements, voy. C. FORGET, « La protection des données dans le secteur de la "police" et de la justice », in V. FRANSEN et D. FLORE, *Société numérique et droit pénal - Belgique, France, Europe, Bruxelles*, Bruylant, 2019, pp. 327-366 ; C. FORGET, « Titre 20 - La protection des données dans le secteur de la "police" et de la "justice" », in *Le règlement général sur la protection des données (RGPD/GDPR)*, Bruxelles, Larcier, 2018, pp. 865-900 ; P. DE HERT et V. PAPAKONSTANTINOU, « The new police and criminal justice data protection directive. A first analysis », *N.J.E.C.L.*, 2016, pp. 7-19.

⁸ Entendu au sens de l'article 4, 2), du RGPD : il s'agit, en effet, de « toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction des données ». Art. 26, 2^o, de la loi.

⁹ Art. 27 de la loi.

émeutes, les activités guidées par des éléments qui ne permettent pas de savoir au préalable si l'incident justifiant l'intervention de la police constitue une infraction pénale ou non, les activités de la police dans le cadre de l'application de sanctions administratives communales¹⁰. Sont donc concernées les données récoltées sur les supporteurs, les mendiants qui seraient à l'origine de nuisances, les personnes actives en ligne¹¹... Le champ d'application de la loi est néanmoins bien plus large puisque, conformément à la directive, les données traitées dans le cadre des enquêtes, des poursuites et de l'exécution des peines sont également visées¹².

b) Les « autorités compétentes »

Les autorités qui sont tenues au respect de la protection des données personnelles renvoient à de multiples instances ayant exclusivement ou essentiellement des compétences en matière de recherche, de détection et de poursuites des infractions pénales : les services de police, les autorités judiciaires (les cours et tribunaux – soit les magistrats, les juridictions, les greffes et les collèges – et le ministère public, en ce compris les collèges tels que le Collège des procureurs généraux¹³), le service d'enquête du comité permanent de contrôle des services de police (Comité P)¹⁴, le service d'enquête du comité permanent de contrôle des services de renseignements (Comité R)¹⁵, l'Inspection générale de la police fédérale et de la police locale, l'Administration générale des douanes et accises¹⁶, l'Unité d'information des passagers¹⁷, et la Cellule de traitement des informations financières¹⁸. Il peut également s'agir de sous-traitants¹⁹ amenés à exercer certaines missions de nature pénale – par exemple, assurer la gestion d'un établissement pénitentiaire²⁰ – sur la base d'un contrat conclu avec les autorités publiques, dont l'exécution les amène à traiter des données personnelles aux fins pénales précitées²¹.

Ces « autorités compétentes » sont par contre soumises au RGPD lorsqu'elles traitent de données personnelles à d'autres fins que celles précisées dans la loi (par exemple, s'agissant des données récoltées dans le cadre des ressources humaines des services de police)²². Par ailleurs, il peut arriver que d'autres autorités – non visées par la loi – exercent des compétences de nature pénale : les

services d'inspection sociale, les services d'inspection économique, les services compétents en matière de contrôle fiscal, la FSMA, les communes... Celles-ci ne sont pas soumises aux dispositions particulières du titre 2 de la loi du 30 juillet 2018. Les travaux préparatoires précisent que c'est dès lors le RGPD qui s'applique au traitement des données personnelles auxquelles elles seraient amenées à se livrer, en tant que régime général²³. La conformité du droit interne avec la directive pourrait néanmoins, sur ce point, susciter quelques difficultés dès lors que celle-ci s'applique à « toute autorité publique compétente pour la prévention et la détection d'infractions pénales, les enquêtes et les poursuites en la matière ou l'exécution de sanctions pénales », ce dont certaines des autorités exclues du champ d'application de la loi sont pourtant chargées.

c) Les données personnelles

Comme le RGPD, la protection mise en place s'applique aux données concernant une personne physique identifiée ou « identifiable »²⁴. *A priori*, la loi ne s'applique donc pas aux informations anonymes ou aux données personnelles rendues anonymes de telle manière que la personne concernée ne soit pas ou plus identifiable²⁵. Ce serait le cas, par exemple, pour les données relatives à l'auteur d'une dénonciation anonyme que la police recevrait concernant la commission d'une infraction. Par contre, les données récoltées à l'occasion d'un témoignage anonyme ne sont pas visées, l'identité du témoin étant « tenue secrète » par le juge d'instruction qui disposera donc de certaines données permettant d'identifier ledit témoin²⁶.

2. Droits d'information, d'accès et de rectification

Bien que la protection des données personnelles soit un principe transversal du droit de l'Union européenne²⁷, le traitement d'informations par la police et les autorités judiciaires participe de la politique européenne de créer un Espace de liberté, de sécurité et de justice, au contraire du RGPD qui contribue à la création d'un marché unique des données. Les garanties offertes aux personnes concernées par la directive, ainsi que sa transposition en droit belge, sont ainsi plus limitées. Nous examinons ici les droits d'information (a), d'accès (b) et de rectification (c) dont les

¹⁰ Considérant n° 12 de la directive. Voy. aussi exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2017-2018, n° 54-3126/001, pp. 67-69.

¹¹ *Ibid.*, p. 69.

¹² La loi encadre ainsi le traitement des données personnelles relatives aux condamnations pénales et aux infractions ou aux mesures de sûreté connexes dont le RGPD précisait qu'il ne pouvait être effectué que sous le contrôle de l'autorité publique ou moyennant certaines garanties. Voy. art. 10 du RGPD.

¹³ Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2017-2018, n° 54-3126/001, p. 60.

¹⁴ Précisément dans le cadre des missions d'enquête qui lui sont dévolues par l'article 16, alinéa 3, de la loi organique du 18 juillet 1991 du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace, *M.B.*, 26 juillet 1991.

¹⁵ Précisément dans le cadre des missions d'enquête qui lui sont dévolues par l'article 40, alinéa 3, de la loi précitée du 18 juillet 1991, lorsqu'elles sont effectuées à charge des membres des services de renseignement, de l'OCAM ou d'autres services d'appui en matière de transmission d'informations utiles à l'analyse de la menace.

¹⁶ Dans le cadre de ses missions de recherche, constatation et de poursuites des infractions déterminées par la loi générale sur les douanes et accises du 18 juillet 1977 et par la loi du 22 avril 2003 octroyant la qualité d'officier de police judiciaire à certains agents de l'Administration générale des douanes et accises. Pour plus d'informations sur ses missions, voy. exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2017-2018, n° 54-3126/001, pp. 61-62.

¹⁷ Créée, au sein du SPF Intérieur, spécifiquement en vue de la collecte, de la conservation, du traitement et de l'échange des données des passagers transmises par les transporteurs et les opérateurs de voyage, laquelle analyse

ces données avant l'arrivée, le transit ou le départ d'une personne sur le territoire national. Voy. le chapitre 7 de la loi du 25 décembre 2016 relative au traitement des données des passagers, *M.B.*, 25 janvier 2017. La loi ne s'applique que lorsque les données sont traitées dans le cadre d'une finalité pénale (soit les finalités visées à l'art. 8, § 1^{er}, 1^o, 2^o, 3^o, 5^o, de ladite loi).

¹⁸ Art. 26, 7^o, de la loi.

¹⁹ Un sous-traitant vise « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement ou d'un autre sous-traitant ». Art. 26, 9^o, de la loi.

²⁰ C. FORGET, « La protection des données dans le secteur de la "police" et de la justice », *op. cit.*, spéc. p. 335.

²¹ Considérant n° 11 de la directive.

²² Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2017-2018, n° 54-3126/001, pp. 58-69. Art. 9, § 2, de la directive.

²³ Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2017-2018, n° 54-3126/001, p. 24.

²⁴ Une personne est réputée identifiable lorsqu'elle peut être identifiée – directement ou indirectement – notamment par référence à un identifiant (un nom, un numéro d'identification, des données de localisation, un identifiant en ligne) ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale. Art. 26, 1^o, de la loi.

²⁵ Considérant n° 21 de la directive.

²⁶ Voy. les art. 86bis à 86quater C.I.Cr.

²⁷ Art. 8 de la Charte des droits fondamentaux et art. 16 du TFUE.

personnes concernées peuvent se prévaloir dans le cadre du traitement de leurs données à des finalités pénales.

a) Droit d'information

Prérequis à l'exercice de leurs autres droits, les personnes concernées par des traitements de données par la police, les autorités judiciaires ou les autres autorités visées par la loi disposent du droit à être informées que leurs données sont collectées et traitées, en ce compris si la collecte est, dans un premier temps, effectuée à l'insu des personnes concernées. Cette information peut toutefois être retardée, limitée ou exclue par la loi pour éviter de gêner les enquêtes et les procédures pénales ou de nuire à la prévention ou à la détection d'infractions pénales²⁸. À cet égard, les cours et tribunaux ainsi que le ministère public restent prioritairement tenus par les dispositions du Code judiciaire, du Code d'instruction criminelle et des lois particulières relatives à la procédure pénale dont les règles s'appliqueront prioritairement en tant que *lex specialis*²⁹.

Cette position s'explique : il est nécessaire d'assurer l'effectivité des mesures de collecte de données, tandis qu'une notification, même celle qui porterait sur le seul fait que des données ont été récoltées, pourrait avoir des répercussions plusieurs années plus tard, par exemple si une enquête n'est pas encore achevée et requiert que de nouvelles mesures de collecte de données soient prises à l'égard des mêmes individus.

Toutefois, selon la jurisprudence de la Cour européenne des droits de l'homme, une personne qui soupçonnerait faire l'objet d'une mesure de collecte de données devrait disposer d'un recours afin d'obtenir confirmation qu'une telle mesure a été prise (ou non) à son égard, et d'éventuellement pouvoir exercer les droits qui en découlent³⁰.

Le droit à l'information dans le contexte de la loi belge requiert notamment de communiquer à la personne concernée le nom du responsable de traitement, l'existence d'un droit d'accès et de rectification des données personnelles récoltées, les finalités poursuivies par le traitement, la base juridique de celui-ci, et la durée de conservation des données³¹.

La loi prévoit également que les brèches de sécurité qui pourraient engendrer un risque élevé pour les droits et libertés d'une personne concernée doivent être notifiées à celle-ci³². Les autres brèches ne doivent pas être notifiées³³.

b) Droit d'accès

S'agissant du droit d'accès, par analogie avec le RGPD³⁴, la directive souhaite respecter prioritairement les règles existant par ailleurs en matière d'accès aux documents officiels³⁵. Cette question est actuellement réglée au niveau

européen par la directive sur la réutilisation des informations du secteur public³⁶, mais fera l'objet d'une nouvelle réglementation à partir de 2021³⁷. Les deux instruments excluent de leur champ d'application les documents non accessibles en vue de protéger la sécurité publique³⁸. À l'égard des données traitées par la police et les autorités judiciaires, c'est donc une règle contraire à celle applicable en matière d'accès aux documents officiels dans un cadre économique ou politique qui est d'application : l'accès est par défaut exclu. La directive relative au traitement des données par la police et les autorités judiciaires vise néanmoins des situations où le droit d'accès doit être garanti³⁹.

Aussi, la loi du 30 juillet 2018 prévoit-elle un droit d'accès aux données de même que la possibilité d'obtenir une confirmation qu'aucune donnée n'est traitée ainsi qu'un accès aux les informations disponibles quant à la source de ces données⁴⁰. L'exercice de ce droit peut être limité entièrement ou partiellement, pour des raisons similaires à celles déjà évoquées pour le droit à l'information. Une telle limitation requiert néanmoins une intervention législative, en vue de respecter les droits fondamentaux, dont les droits de la défense⁴¹. Les droits d'accès varient selon le stade de la procédure pénale.

Au stade de l'information et de l'instruction, le Code d'instruction criminelle prévoit que toute personne intéressée peut demander l'accès et obtenir une copie d'un dossier pénal qui la concerne auprès du procureur du Roi ou du juge d'instruction. La possibilité d'accéder au dossier répressif a été fortement élargie à la fin des années 1990, dans le cadre de la réforme du « petit Franchimont » qui visait à instaurer davantage d'éléments contradictoires au stade de l'enquête pénale⁴².

Cette possibilité de demander l'accès au dossier répressif ne correspond pas exactement au droit d'accès aux données conféré sous l'empire de la loi de 2018 : entre données collectées et dossier pénal, la portée du droit peut comprendre soit *plus d'informations* (la victime qui aurait accès à toutes les informations sur le prévenu dans le cadre d'une même affaire), soit moins d'informations (le prévenu n'a pas accès à toutes les informations que la police détient sur un témoin).

Sont visés par la notion de personnes intéressées notamment l'inculpé, la personne à l'égard de laquelle l'action publique est engagée dans le cadre de l'instruction, la personne soupçonnée, la partie civilement responsable, la partie civile, celui qui a fait une déclaration de personne lésée, le curateur ou l'administrateur provisoire⁴³. Cette liste distingue plusieurs catégories de personnes, dont les intérêts divergent. Cette distinction peut ainsi justifier que l'accès pour un même dossier puisse être octroyé pour une victime plus aisément que pour une personne

²⁸ Art. 37, § 2, de la loi.

²⁹ Art. 37, § 4, de la loi. Voy. aussi P. DE HERT et V. PAPAKONSTANTINOU, « The new police and criminal justice data protection directive. A first analysis », op. cit., spéc. p. 9.

³⁰ Cour eur. D.H., 18 mai 2010, n° 26839/05, *Kennedy c. Royaume-Uni*, §§ 124 et 167. Voy. également Cour eur. D.H., 4 décembre 2015, *Zakharov c. Russie*, §§ 169 et 171.

³¹ Art. 37, § 1^{er}, de la loi.

³² Art. 62, § 1^{er}, C.I.Cr.

³³ Art. 62, § 3, C.I.Cr.

³⁴ Considérant 154 et art. 86 du RGPD.

³⁵ Considérant 16 de la directive (UE) 2016/680.

³⁶ Directive 2003/98/CE du Parlement européen et du Conseil du 17 novembre 2003 concernant la réutilisation des informations du secteur public, *J.O.U.E.*, n° L 345 du 21 décembre 2003, pp. 90 et s.

³⁷ Directive (UE) 2019/1024 du Parlement européen et du Conseil du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public (refonte), *J.O.U.E.*, n° L 172 du 26 juin 2019, pp. 56 et s.

³⁸ Art. 1^{er}, § 2, c, de la directive 2003/98/CE, et art. 1^{er}, § 2, d, de la directive (UE) 2019/1024.

³⁹ Art. 13 à 16 de la directive (UE) 2016/680.

⁴⁰ Art. 38, § 1^{er}, de la loi.

⁴¹ Art. 38, § 2, de la loi.

⁴² Fr. KONING, « Reconnaissance du droit du citoyen de refuser de donner accès à un système informatique nonobstant l'ordre de la loi, et reconnaissance d'un droit de recours contre un refus du parquet de laisser consulter son dossier d'information », *J.L.M.B.*, 2016/16, p. 742.

⁴³ Art. 21bis, § 1^{er}, al. 2 et 61ter, § 2, C.I.Cr.

soupçonnée d'une infraction.

En outre, cette distinction correspond, dans une large mesure, à la distinction que le responsable du traitement des données doit réaliser dans le cadre de la collecte de données à des fins pénales. Il doit en effet séparer, pour autant que faire se peut, les données des personnes à l'égard desquelles il existe des motifs sérieux de croire qu'elles ont commis ou sont sur le point de commettre une infraction pénale, les personnes reconnues coupables d'une infraction pénale, les victimes d'une infraction pénale et les tiers à une infraction pénale, tels que les personnes pouvant être appelées à témoigner ou des associés des personnes soupçonnées d'avoir commis une infraction⁴⁴. Cette distinction est importante : la personne concernée par le traitement de ses données ne devrait pouvoir accéder à ces dernières que pour assurer le respect de ses droits, non pour collecter des informations sur des tiers. Ainsi, il ne faudrait pas qu'une personne soupçonnée d'avoir commis une infraction puisse utiliser ce droit d'accès pour contacter et intimider les témoins ou les victimes (ou inversement).

Comme la loi du 30 juillet 2018, le Code d'instruction criminelle fixe également les limites de ce droit de solliciter l'accès au dossier répressif⁴⁵. Pour obtenir l'accès au dossier pénal, la personne doit accompagner sa demande d'une motivation légitime et démontrer son intérêt. Le procureur du Roi (ou le juge d'instruction) peut limiter l'accès au dossier essentiellement lorsque la consultation est contraire aux nécessités de l'enquête, qu'elle présente un danger pour les personnes ou qu'elle porte gravement atteinte à la vie privée de tiers⁴⁶. Le requérant peut introduire un recours à l'encontre d'une décision de refus ou de limitation d'accès devant la chambre des mises en accusation⁴⁷.

Après la clôture de l'information ou de l'instruction, c'est-à-dire lorsqu'est saisie la juridiction de jugement chargée de statuer sur les infractions pénales commises, le prévenu et la victime ont automatiquement accès au dossier répressif – et aux données qu'il contient – sans restriction⁴⁸.

c) Droits de rectification et de complétion

La loi du 30 juillet 2018 prévoit que les données récoltées à des fins pénales peuvent être rectifiées ou complétées si elles sont inexactes. Ces droits sont soumis aux contraintes déjà énoncées et liées aux nécessités de recherche d'infractions, des enquêtes et, plus généralement, des procédures pénales. Le responsable du traitement doit

effacer les données qui n'auraient pas été collectées de façon licite, ou qui seraient utilisées en dehors des finalités de traitement prévues par la loi.

Néanmoins, si la personne concernée conteste l'exactitude des informations mais que cette exactitude ne peut être vérifiée, les données ne seront pas nécessairement effacées : le traitement en sera uniquement limité. Si la limitation du traitement devait être levée (permettant ainsi de transmettre les informations à d'autres services de police, par exemple dans le cadre de la recherche d'autres infractions pénales), le responsable de traitement en informera la personne concernée⁴⁹.

En outre, et de manière analogue au RGPD⁵⁰, la directive⁵¹ et la loi du 30 juillet 2018⁵² permettent de compléter les données, renforçant ainsi les droits de la personne concernée. Ce droit peut être exercé notamment sous la forme d'une déclaration complémentaire. Il s'agit du principal mécanisme qui permet de nuancer des données qui concernent plusieurs personnes (par exemple l'auteur de l'infraction mais également la victime ou le verbalisant)⁵³, sans affecter les données des autres personnes. Par ailleurs, pour assurer l'effectivité de ces droits, les autorités compétentes doivent distinguer clairement ce qui relève du fait de ce qui relève de l'appréciation personnelle de la victime ou du verbalisant.

3. Une autorité de contrôle spécifique : l'Organe de contrôle de l'information policière (le COC)

Si les États membres avaient la possibilité de désigner, en tant qu'autorité de contrôle des dispositions spécifiques au traitement des données dans le domaine pénal, la même autorité que celle instituée en vertu du RGPD⁵⁴ (soit principalement, en Belgique, l'Autorité de protection des données⁵⁵, ci-après « APD »), ce n'est pas l'option qui a été choisie par le législateur belge. Celui-ci a, en effet, préféré répartir la compétence de contrôle entre diverses entités en fonction des autorités amenées à traiter des données personnelles à des fins pénales.

Ainsi, si le traitement des données est le fait des services de police, de l'Inspection générale de la police fédérale et locale, de l'Unité d'information des passagers⁵⁶, ou de l'Administration générale des douanes et accises (spécifiquement lorsque celle-ci sollicite, dans le cadre de l'exercice de ses missions, certaines données auprès de l'Unité d'information des passagers)⁵⁷, l'autorité de contrôle compétente est l'Organe de contrôle de l'information policière⁵⁸.

⁴⁴ Art. 31 de la loi.

⁴⁵ Ces restrictions sont modalisées au stade l'information (art. 21bis C.I.Cr.) et de l'instruction (art. 61ter C.I.Cr.).

⁴⁶ Art. 21bis, § 5, et 61ter, § 3, C.I.Cr.

⁴⁷ Ce recours a été introduit, s'agissant de l'accès au dossier au cours de l'information, après que la Cour constitutionnelle a censuré, par un arrêt n°6/2017 du 25 janvier 2017, la loi du 27 décembre 2012 portant des dispositions diverses (M.B., 31 janvier 2013). En effet, la Cour a estimé qu'il y avait une discrimination non justifiée entre la phase d'information, à l'égard de laquelle aucun recours n'était prévu, et la phase d'instruction, qui permettait au requérant l'exercice d'un recours.

⁴⁸ Voy. G. FALQUE, « La victime dans le débat pénal », in P. CHOME, O. KLEES et A. LORENT (dir.), *Droit pénal et de la procédure pénale*, supplément n° 47, octobre 2018, Malines, Kluwer, §§ 237 et s., 286 et s., 337 et s.

⁴⁹ Art. 39 de la loi.

⁵⁰ Art. 16 du RGPD.

⁵¹ Art. 14 de la directive

⁵² Art. 39, § 1^{er}, de la loi.

⁵³ P. VOIGT et A. VON DEM BUSCHKE, *The EU General Data Protection Regulation (GDPR) : A Practical Guide*, 1^{re} éd., Springer, Cham (Suisse), 2017, pp. 155-156.

⁵⁴ Art. 41, § 3, de la directive.

⁵⁵ Telle qu'elle a été instituée par la loi du 3 décembre 2017 portant création de l'Autorité de protection des données, M.B., 10 janvier 2018.

⁵⁶ Uniquement lorsque celle-ci traite des données à des fins pénales, à l'exclusion des données qu'elle traite aux fins du suivi des activités de renseignement et de sécurité. Dans ce cas, l'autorité de contrôle compétente est le Comité R. Voy. l'article 184 lu en combinaison avec l'article 169 de la loi.

⁵⁷ Soit les missions exercées par l'Administration en vue de rechercher les crimes et délits visés à l'article 8, § 1^{er}, 5^o, de la loi du 25 décembre 2016 relative au traitement des données des passagers.

⁵⁸ Art. 71, § 1^{er}, al. 3, de la loi. Voy. aussi Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2017-2018, n° 54-3126/001, p. 10.

Le COC est, depuis 2014⁵⁹, l'institution de référence⁶⁰ pour le contrôle de la gestion de l'ensemble de l'information policière, données personnelles incluses⁶¹. La loi du 30 juillet 2018 dote le COC d'un cadre juridique propre. Cette loi a revu, redéfini et rationalisé sa structure, sa composition, le statut de ses membres, leurs missions et leurs compétences, non seulement en conformité avec la directive, mais aussi sur la base de l'expérience acquise par l'organe de contrôle depuis 2014⁶².

a) Missions

Pour l'heure, en vertu de la loi du 30 juillet 2014, le COC est chargé de surveiller l'application du titre II de ladite loi, de contrôler le traitement des informations et des données à caractère personnel traitées par les services de police⁶³ outre les autres missions qui lui sont déjà confiées par ou en vertu d'autres lois⁶⁴. La loi confie également au COC la mission d'émettre des avis sur toute question relative à la gestion de l'information policière ou de veiller à la légalité du contenu des banques de données policières⁶⁵. Le COC est aussi l'instance compétente pour recevoir des plaintes et en assurer le traitement et le suivi⁶⁶. D'autres missions, compatibles avec celles d'une APD, ne sont pas à exclure à l'avenir, telles que, par exemple, le contrôle du respect des conditions en vue de l'installation et de l'utilisation de caméras à des fins policières⁶⁷.

Le COC peut compter, pour l'exercice de ses missions, sur un service d'enquête pouvant procéder à l'exécution de divers devoirs, tels que procéder à l'audition de personnes⁶⁸, accéder de manière illimitée aux informations et aux données traitées par les services contrôlés, ainsi qu'aux locaux où se trouvent ces données, y saisir tous les objets, documents ou données d'un système informatique utiles à l'enquête, à l'exception de ceux concernant une information ou une instruction judiciaire en cours, et ce, si besoin, en requérant l'assistance de la force publique⁶⁹.

b) L'Autorité de protection des données : une intervention résiduaire dans le cadre du traitement des données à des fins pénales

L'APD constitue l'autorité de contrôle résiduaire, pour tous les autres traitements de données personnelles à finalités pénales⁷⁰, tels que ceux effectués par les services d'enquête du Comité P et du Comité R⁷¹, et, sauf l'exception

précitée, par l'Administration générale sur les douanes et accises⁷².

c) L'indépendance du ministère public et du pouvoir judiciaire

Il faut souligner que les cours et tribunaux et le ministère public ne sont quant à eux soumis, dans le cadre de l'exercice de leur fonction juridictionnelle⁷³, à aucune autorité de contrôle⁷⁴. Il s'agit, en effet, de préserver l'indépendance du pouvoir judiciaire dans l'accomplissement de ses missions, en ce compris lorsqu'il prend des décisions. La législation belge a utilisé la marge de manœuvre laissée, à cet égard, par l'article 55 du RGPD⁷⁵ pour étendre cette disposition au ministère public à l'égard de l'ensemble de ses missions⁷⁶. Ceci n'empêche néanmoins pas que les parquets et les cours et tribunaux devront, comme tous les autres services de l'État, fournir au COC tous les renseignements utiles à l'exercice de ses missions, éventuellement moyennant autorisation du ministère public compétent si ceux-ci font partie d'une enquête pénale ou judiciaire en cours⁷⁷.

En bref, le traitement de données dans le cadre de finalités pénales constitue donc un silo à part entière, avec des bases légales distinctes. Les personnes concernées par de tels traitements veilleront ainsi à examiner séparément les situations couvertes spécialement par la loi belge et la directive de la protection offerte par défaut par le RGPD. Aussi donneront-elles une attention particulière aux mécanismes de mise en œuvre de ces droits qui requièrent une mise en balance de logiques non économiques : transparence de la mise en œuvre de l'action publique, secret nécessaire des enquêtes, indépendance des magistrats et protection des données personnelles.

■ **Mona Giacometti**

Avocate au barreau de Bruxelles (Juxta Legal)
Maître de conférence (ULiège), assistante
et doctorante (UCLouvain)

■ **Enguerrand Marique**

Chercheur et doctorant (UCLouvain)

⁵⁹ Voy. le chapitre VIIter de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard du traitement des données à caractère personnel, tel qu'inséré par la loi du 18 mars 2014 relative à la gestion de l'information policière, M.B., 28 mars 2014. L'Organe est néanmoins devenu opérationnel en octobre 2015. Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2017-2018, n° 54-3126/001, p. 120.

⁶⁰ Voy. C. const., arrêt du 14 juillet 2016, n° 108/2016. La Cour a balayé tout doute d'inconstitutionnalité par rapport à la loi sur la gestion de l'information policière en faisant référence au rôle crucial joué par le COC.

⁶¹ Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2017-2018, n° 54-3126/001, p. 116.

⁶² Voy. les art. 231 à 251 de la loi. Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2017-2018, n° 54-3126/001, pp. 118-121.

⁶³ Précisément les données visées aux articles 44/1 à 44/11/13 de la loi du 5 août 1992 sur la fonction de police, M.B., 22 décembre 1992.

⁶⁴ Art. 71, § 1^{er}, al. 3, de la loi.

⁶⁵ Art. 236 à 243 de la loi.

⁶⁶ Art. 240, 4^e, de la loi.

⁶⁷ Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2017-2018, n° 54-3126/001, p. 123.

⁶⁸ Art. 245 de la loi.

⁶⁹ Art. 244 de la loi.

⁷⁰ Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2017-2018, n° 54-3126/001, p. 11.

Art. 4, § 2, al. 2, de la loi du 3 décembre 2017 portant création de l'Autorité de protection des données, M.B., 10 janvier 2018.

⁷¹ Les Comités P et R ont été institués comme autorités de protection des données essentiellement pour les services de renseignement et de sécurité (Comité R) et de l'OCAM (Comités P et R). Ils ne sauraient toutefois intervenir comme autorités de contrôle de leurs propres services d'enquête sous peine de porter atteinte à l'exigence d'indépendance qui doit nécessairement caractériser l'autorité de contrôle. Voy. art. 41, § 1^{er}, de la directive.

⁷² C. FORGET, « La protection des données dans le secteur de la "police" et de la justice », *op. cit.*, spéc. p. 360.

⁷³ Entendu au sens large, et comprenant, par exemple, le traitement de données dans le cadre de la gestion du personnel des autorités judiciaires. Projet de loi portant création de l'Autorité de protection des données, exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2016-2017, p. 14.

⁷⁴ Exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2017-2018, n° 54-3126/001, p. 229. Voy. aussi art. 4, § 2, al. 1^{er}, de la loi du 2 décembre 2017 portant création de l'Autorité de protection des données.

⁷⁵ Voy. aussi les considérants n° 20 du RGPD et n° 80 de la directive.

⁷⁶ Projet de loi portant création de l'Autorité de protection des données, exposé des motifs, *Doc. parl.*, Ch. repr., sess. ord. 2016-2017, pp. 13-14.

⁷⁷ Art. 246 de la loi. À notre sens, même si la loi ne le prévoit pas expressément, rien ne s'oppose, en cas de refus du ministère public, que le COC introduise un recours auprès de la chambre des mises en accusation conformément aux dispositions de l'article 21bis, §§ 7 et 8, du C.I.Cr.