UCLouvain

Faculté de droit et de criminologie

Europol : comment peut-on combiner le recueil et le traitement massif d'informations avec la protection des données à caractère personnel ?

Auteur : Sophia Babatzikis
Promoteur : Daniel Flore
Lecteur(s) : /
Année académique 2020-2021
Master en Droit finalité Justice civile et pénale

Plagiat et erreur méthodologique grave

Le plagiat, fût-il de texte non soumis à droit d'auteur, entraîne l'application de la section 7 des articles 87 à 90 du règlement général des études et des examens.

Le plagiat consiste à utiliser des idées, un texte ou une œuvre, même partiellement, sans en mentionner précisément le nom de l'auteur et la source au moment et à l'endroit exact de chaque utilisation*.

En outre, la reproduction littérale de passages d'une œuvre sans les placer entre guillemets, quand bien même l'auteur et la source de cette œuvre seraient mentionnés, constitue une erreur méthodologique grave pouvant entraîner l'échec.

* A ce sujet, voy. notamment **http://www.uclouvain.be/plagiat**.

REMERCIEMENTS

Je souhaite avant tout remercier Monsieur Daniel FLORE, mon promoteur, pour son temps et son aide précieuse au cours de ces deux dernières années. Merci de m'avoir laissé écrire mon mémoire sur un sujet qui me tenais à cœur.

Je remercie ensuite chaleureusement Monsieur Pieter-Jan DE GRAVE, l'officier en charge de la protection des données au sein de la police fédérale belge, pour son amabilité, son temps et l'intérêt qu'il a porté à mon mémoire. Notre entretien m'a été d'une grande aide dans l'élaboration de ce travail.

Je remercie également Monsieur Daniel DREWER, l'officier en charge de la protection des données au sein d'Europol, pour ses connaissances et son expérience du milieu qu'il a partagées avec moi.

Je tenais à adresser un remerciement particulier à ma grand-mère, Sophia PANTZIDIS, pour sa patience, sa disponibilité et surtout ses judicieux conseils d'orthographe qui ont contribué à bonifier mon mémoire.

Pour terminer, j'adresse mes sincères remerciements à tous ceux qui, de près ou de loin, m'ont apporté leur aide et leur soutien lors de la réalisation de ce mémoire.

Table des matières

INTRODUCTION

Au sein de l'Union européenne, la protection des données à caractère personnel est, depuis longtemps, reconnue comme un élément primordial nécessitant une protection particulière. Considéré au départ, comme un simple aspect du droit à la vie privée, la protection des données à su démontrer son importance et se hisser au rang des droits fondamentaux[1]. Reconnu explicitement dans plusieurs instruments juridiques, tels que dans l'article 16 du Traité sur le fonctionnement de l'Union européenne et l'article 8 de la Charte des droits fondamentaux de l'Union européenne, la protection des données personnelles fait désormais partie intégrante de la catégorie des droits de l'Homme. Aujourd'hui plus que jamais, le droit à la protection des données personnelles fait l'objet de nombreux sujets d'actualité.

Dans ce contexte et à l'ère du numérique, l'interaction entre la protection des données personnelles et les développements technologiques permettant, entre autres, le traitement d'un large volume de données, est essentiel pour une agence de l'Union européenne telle qu'Europol qui traite un nombre grandissant de données personnelles[2]. L'objectif principal de ce mémoire est d'analyser et de comprendre comment Europol combine le recueil massif d'informations dont il dispose, tout en garantissant le respect de la protection des données personnelles, pour combattre les formes graves de criminalité et le terrorisme au sein de l'Union européenne. Le paradoxe qui existe entre le respect du droit fondamental qu'est celui de la protection des données personnelles et le besoin d'adopter, pour des raisons de sécurité publique, des techniques permettant la collecte et le traitement massif de données, est le fil rouge de ce mémoire.

Europol[3], véritable plaque tournante pour les informations criminelles, a été bâti sur les bases de la confidentialité afin de permettre à la police d'être efficace lors de ses enquêtes criminelles. À l'origine, l'Office européen de police manquait cruellement de transparence autour de la gestion du traitement des données personnelles dont il disposait. Aujourd'hui, grâce à la mise en place d'un

[1] T. MARQUENIE, « The Police and Criminal Justice Authorities Directive: Data protection standards and impact on the legal framework », *Computer Law & Security Review*, vol. 33, 2017, p. 324.
[2] D. DREWER et V. MILADINOVA, « The BIG DATA Challenge: Impact and opportunity of large quantities of information under the Europol Regulation », *Computer Law & Security Review*, vol. 33, 2017, p. 298.
[3] « L'Office européen de police » ou « l'agence de l'Union européenne » sont également des termes utilisés pour désigner Europol.

contrôle parlementaire au nom de l'État de droit[4], la collecte et le traitement qu'Europol fait des données personnelles sont de moins en moins opaques.

À sa création, l'Office européen de police était une agence intergouvernementale financée par les contributions des États-membres dont la mission principale était de coordonner, entre les services répressifs nationaux, l'échange d'informations en matière de stupéfiants[5]. Europol a ensuite évolué et est devenu, en 2009, une agence de l'Union européenne à part entière. Afin de s'adapter aux évolutions sociétales et technologiques ainsi qu'à la diversification des formes de criminalité, Europol a connu, en moins de trente ans, une Convention, une décision du Conseil et enfin un règlement. À cette liste s'ajoutera bientôt un nouveau règlement, suite à une proposition de modification du règlement Europol par le Parlement européen et le Conseil.

La première partie de ce mémoire sera entièrement consacrée aux généralités entourant l'Office européen de police et au règlement (UE) 2016/794 du 11 mai 2016 relatif à l'agence de l'Union européenne pour la coopération des services répressifs. Nous commencerons par analyser le statut, les missions, la structure et la gouvernance d'Europol afin d'en comprendre son fonctionnement. Concernant le règlement Europol, nous aborderons deux sujets ; d'une part, la façon dont l'Office collecte, traite et stocke les données à caractère personnel qu'il détient et, d'autre part, la coopération existante avec les États-membres ainsi que la collaboration avec des parties privées. Nous verrons que les États-membres n'ont pas d'obligations, *stricto sensu,* de transmettre des informations à Europol, ce qui signifie qu'ils sont libres de coopérer ou non avec l'agence. Dans le passé, cette liberté de choix a porté préjudice à Europol qui souffrait véritablement d'un manque d'informations venant des services répressifs nationaux, réticents face à une collaboration avec l'agence. Enfin, nous verrons également que l'échange de données opérationnelles avec des parties privées, soulève de véritables questions vis-à-vis du respect de certains droits fondamentaux et expose les limites du cadre juridique, actuellement applicable, régissant la coopération entre l'agence et des parties privées.

La deuxième partie de ce mémoire sera consacrée aux définitions des termes « données à caractère personnel » et « traitement des données ». Ces deux notions sont abordées tout au long

[4] P. BERTHELET, « Europol à l'épreuve du secret. Dépassement du modèle intergouvernemental, respect de l'État de droit et accroissement du contrôle démocratique », *OpenEdition*, 2019, pp.5-6.
[5] E. DAVID, « Chapitre VI - La coopération judiciaire et pénale en matière d'enquête et d'instruction » in *Éléments de droit pénal international et européen* (sous la dir. de E. DAVID), 2e édition, Bruxelles, Bruylant, 2018, pp. 443-444.

de ce mémoire et nous avons jugé indispensables de les définir pour comprendre le sens de ce travail. Nous aborderons également les objectifs de la mise en place du règlement général sur la protection des données, plus connu sous le nom de RGPD. Bien qu'elle ne s'applique pas à Europol, cette réglementation exerce une influence importante sur l'efficacité de ses activités, notamment en matière de cybercriminalité. Nous verrons en effet que cette évolution législative a des impacts majeurs pour les services répressifs de l'Union européenne comme celui de la perte de données.

La troisième partie analysera ensuite le défi que représente le *Big data*[6] pour Europol, pris au sens de l'amplification et de l'accélération du processus de collecte, de traitement et d'échange de données à l'échelon transnational. De nos jours, le phénomène du *Big data* est devenu un sujet majeur de débat dans les domaines de l'application de la loi et de la sécurité nationale[7]. Le traitement d'une quantité accrue de données à caractère personnel pose, en effet, de véritables défis quant à la protection de ces mêmes données et au regard du droit à la vie privée des citoyens ; deux droits qui ont été élevés au rang de droits de l'Homme [8]. Successivement, des questions relatives à l'émergence du *Big data*, aux dangers potentiels qu'il représente ainsi qu'au dilemme complexe que son traitement soulève au sein d'Europol, seront abordées. Nous verrons la complexité qui se cache derrière le défi du *Big data,* à savoir cette lutte constante entre la vie privée des citoyens et le besoin d'augmenter la sécurité en Europe. Enfin, nous ferons part de l'inquiétude de la Ligue des droits de l'Homme et d'autres collectifs citoyens face au danger d'une potentielle surveillance de masse que représente le traitement d'une large quantité de données personnelles à l'échelle transnationale.

Pour finir, nous analyserons la proposition de modification du règlement Europol ainsi que les commentaires du Contrôleur européen de la protection des données et du Conseil des barreaux européens, à l'égard de cette initiative législative. La quasi-totalité des révisions abordées au sein

[6] *Big data* signifie littéralement méga-données ou données massives. C'est un ensemble de données - qu'elles soient à caractère personnel ou non - qui en raison de leur volume ou de leur nature, sont difficilement traitable à l'aide d'une base de données standard.
[7] D. DREWER et V. MILADINOVA, *opcit.*, p. 299.
[8] C. de TERWANGNE, « Chapitre 9. - Internet et la protection de la vie privée et des données à caractère personnel » *in L'Europe des droits de l'homme à l'heure d'Internet* (sous la dir. de C. de TERWANGNE et Q. Van ENIS), 1e édition, Bruxelles, Bruylant, 2019, p. 325-368.

de cette proposition impliquent le traitement des données à caractère personnel par Europol. Par conséquent, nous avons jugé pertinent de l'analyser, également, dans le cadre de ce mémoire.

Nous avons choisi d'écrire notre mémoire de fin d'études sur la confidentialité et la protection des données personnelles, un sujet actuellement au cœur des préoccupations sociétales actuelles. Pour étayer notre travail et compléter notre partie théorique sur le fonctionnement et l'organisation d'Europol, en lien avec le traitement des données, nous avons interrogé le *Data Protection Officer* de la police fédérale belge, Monsieur Pieter-Jan De Grave ainsi que le *Data Protection Officer* d'Europol, Monsieur Daniel Drewer. Ils nous ont apporté leurs points de vue, nous permettant ainsi de fournir un travail complet et qualitatif.

PARTIE 1 : EUROPOL

Chapitre 1 : Bref historique des bases légales

L'émergence de l'Office européen de police s'inscrit dans un contexte global de mondialisation et d'évolution de la criminalité transnationale. Le souhait de créer une « Europe de la sécurité » découle d'une volonté politique exprimée par les dirigeants européens, tels François Mitterrand et Helmut Kohl[9]. À sa création, Europol était une agence intergouvernementale financée par les contributions des États-membres dont la mission principale était de coordonner l'échange d'informations en matière de stupéfiants entre les États-membres[10]. Europol qui a trouvé son origine dans l'article K.1.9 du Traité de Maastricht, a connu en moins de trente ans d'existence, une Convention[11], une décision du Conseil[12] et enfin un règlement[13]. À cette liste s'ajoutera bientôt un nouveau règlement étant donné qu'une proposition de modification du règlement Europol[14] est en cours de négociations.

L'Office européen de police a acquis le statut d'agence de l'Union européenne à part entière, avec l'entrée en application de la décision du Conseil 2009/371/JAI du 6 avril 2009 portant création de l'Office européen de police. Par conséquent, le budget, le personnel et l'organisation d'Europol, se basent dorénavant sur les règles de l'Union[15]. La décision du Conseil a remplacé la Convention Europol qui était en vigueur depuis le 1er octobre 1998. Les raisons de ce remplacement sont

[9] P. BERTHELET, « Europol face au défi des « méga-données » - L'évolution tendancielle d'une coopération policière européenne « guidée par le renseignement » », *R.D.U.E.*, 2019/2, p.161.
[10] E. DAVID, « Chapitre VI - La coopération judiciaire et pénale en matière d'enquête et d'instruction » in *Éléments de droit pénal international et européen* (sous la dir. de E. DAVID), 2e édition, Bruxelles, Bruylant, 2018, pp. 443-444.
[11] Acte du Conseil du 26 juillet 1995 portant établissement de la convention sur la base de l'article K.3 du traité sur l'Union européenne portant création d'un Office européen de police (convention Europol), *J.O.U.E.*, C 316, 27 novembre 1995.
[12] Décision 2009/371/JAI du Conseil du 6 avril 2009 portant création de l'Office européen de police (Europol), *J.O.U.E.*, L 121, 15 mai 2009.
[13] Règlement (UE) 2016/794/JAI du Parlement européen et du Conseil du 11 mai 2016 relatif à l'agence de l'Union européenne pour la coopération des services répressifs (Europol) et remplaçant et abrogeant les décisions du Conseil 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI et 2009/968/JAI, *J.O.U.E.*, L 135, 24 mai 2016.
[14] Proposition de règlement du Parlement européen et du Conseil modifiant le règlement (UE) 2016/794 en ce qui concerne la coopération d'Europol avec les parties privées, le traitement de données à caractère personnel par Europol à l'appui d'enquêtes pénales et le rôle d'Europol en matière de recherche et d'innovation, COM (2020) 796 final, Bruxelles, 9 décembre 2020.
[15] D. FLORE, *Droit pénal européen : les enjeux d'une justice pénale européenne*, 2e édition, Bruxelles, Larcier, 2014, p. 736.

multiples. Premièrement, la Convention a été jugée comme étant trop rigide et donc inappropriée aux évolutions constantes des menaces criminelles. De plus, la décision a permis d'insérer en son sein les modifications substantielles qui avaient été apportées au champ de compétences matérielles et aux missions d'Europol. Enfin, la décision du Conseil a engendré la simplification et l'amélioration du cadre juridique de l'Office[16]. Bien que le remplacement de la Convention par la décision 2009/371/JAI ait apporté des plus-values à Europol, telle que l'augmentation de sa visibilité au sein des États-membres, la décision du Conseil n'a pas eu pour conséquence de changer la relation de dépendance de l'Office vis-à-vis des États-membres. En effet, les États-membres n'ont pas d'obligation, *stricto sensu*, d'alimenter les bases de données d'Europol en informations, ce qui contraint Europol dans l'exercice de ses fonctions[17].

Dans un souci d'améliorer l'efficacité d'Europol dans son soutien aux services répressifs des États-membres, Le parlement européen et le Conseil ont adopté le règlement Europol, devenu applicable le 1er mai 2017, sur base des articles 87, paragraphe 2, point b) et 88 du traité sur le fonctionnement de l'Union européenne (ci-après « T.F.U.E. »). L'adoption du règlement Europol a eu pour conséquence l'abrogation de la décision du Conseil de 2009. Cette initiative législative a été mis en place afin de poursuivre deux stratégies : à savoir, étoffer la base de données d'Europol en informations venant des États-membres et parallèlement mettre en place un système de traitement des données permettant à Europol de gérer le flux d'informations reçues, afin d'aider pleinement les services répressifs dans leur lutte contre les formes graves de criminalité[18]. Nous aborderons plus en profondeur les raisons de la mise en place du règlement ainsi que ses objectifs, dans le dernier chapitre de cette première partie.

Au vu de la diversification et de l'augmentation des formes de criminalité au sein de l'Union européenne, un nouveau règlement Europol est en cours de négociations. En effet, la Commission européenne a présenté le 9 décembre 2020, une proposition de règlement du Parlement européen et du Conseil, modifiant le règlement (UE) 2016/794 en ce qui concerne la coopération d'Europol avec les parties privées, le traitement de données à caractère personnel par Europol à l'appui

[16] V. AMICI, « Europol et la nouvelle décision du Conseil : entre opportunités et contraintes », *R.D.U.E.*, 2010/1, pp. 80-81.
[17] *Ibid.*, p. 95.
[18] Proposition de règlement du Parlement européen et du Conseil relatif à l'Agence de l'Union européenne pour la coopération et la formation des services répressifs (Europol) et abrogeant les décisions 2009/371/JAI et 2005/681/JAI, COM (2013) 173 final, Bruxelles, 27 mars 2013, p.5.

d'enquêtes pénales et le rôle d'Europol en matière de recherche et d'innovation. Nous examinerons davantage cette proposition dans le dernier chapitre de ce mémoire.

Chapitre 2 : Statut

Europol qui était anciennement une agence intergouvernementale, a acquis le statut d'agence de l'Union européenne en 2009. Cette acquisition a eu de nombreuses conséquences, notamment vis-à-vis du budget alloué à l'Office. Europol se voit concéder un budget propre, alimenté par une contribution du budget général de l'Union européenne[19].

Notons également qu'Europol, dont le siège est fixé à La Haye, est une agence autonome et indépendante dotée de la personnalité juridique[20]. En tant que personne morale, elle dispose d'une large capacité juridique, reconnue par le droit national de chaque État-membre, lui permettant par exemple d'intenter des actions devant les tribunaux et de se défendre lorsqu'elle fait l'objet de poursuites ainsi que d'acquérir des biens immobiliers et mobiliers[21]. La Cour de justice de l'Union européenne est compétente pour connaître de tous litiges contractuels ou extracontractuels mettant en cause la responsabilité d'Europol[22].

Chapitre 3 : Objectifs et Missions

Europol est une agence de l'Union européenne destinée à assister, via des analyses opérationnelles et stratégiques, les services répressifs des États-membres dans leurs enquêtes pénales et à les soutenir dans la prévention des formes graves de criminalité notamment en facilitant l'échange d'informations entre ces derniers. Europol intervient pour répondre à des menaces transnationales, entre autres, parce que l'action individuelle des États-membres, au niveau national, ne suffit pas. L'Office européen de police n'est pas doté de pouvoirs coercitifs[23], ni de capacités d'enquêtes autonomes, ce qui signifie qu'il n'est pas à même de procéder à des mesures exécutives, telles que l'arrestation d'un suspect, sans l'autorisation des autorités nationales, ni d'imposer une

[19] Règlement Europol, considérant n°61.
[20] Règlement Europol, article 62, §1er.
[21] Règlement Europol, article 62, §2.
[22] Règlement Europol, article 49.
[23] Règlement Europol, article 4, §5.

quelconque sanction à un État-membre[24]. Europol est essentiellement un centre d'informations criminelles ; son identification à un « FBI européen » est dès lors inexacte[25].

Les objectifs d'Europol sont listés à l'article 3 du règlement (UE) 2016/794 et nous enseignent que l'Office européen de police va intervenir lorsqu'au moins deux États-membres sont affectés par une forme grave de criminalité ou lors d'une éventuelle attaque terroriste qui constitue une des menaces les plus importantes pour la sécurité de l'Union, ou lorsqu'une forme de criminalité met en péril un intérêt commun faisant l'objet d'une politique européenne[26]. Les formes de criminalité dont il est question, sont listées à l'annexe I dudit règlement et comprennent notamment la lutte contre la criminalité organisée, les activités de blanchiment d'argent, le trafic de stupéfiants, le trafic d'organes et de tissus humains, la criminalité informatique, la corruption et la criminalité au détriment de l'environnement. Les infractions pénales connexes sont également comprises comme étant des objectifs d'Europol[27]. Elles englobent toutes infractions pénales « commises pour se procurer les moyens de perpétrer les actes relevant de la compétence d'Europol, pour en faciliter l'exécution ou les perpétrer ou pour en assurer l'impunité »[28].

L'article 4 du règlement liste les missions d'Europol mises en place afin d'honorer les objectifs de l'Office. Elles comprennent notamment la collecte, le traitement, l'échange et la communication aux États-membres de toutes informations pertinentes, ainsi que la coordination et la réalisation d'enquêtes, dans le but de soutenir les services répressifs des États-membres dans leur lutte contre les formes graves de criminalité[29]. De plus, afin de déterminer les priorités de l'Union concernant la lutte contre les formes graves de criminalité et afin d'utiliser efficacement les ressources mises à disposition par les États-membres et par l'Union européenne, Europol a également pour mission de mettre en place des analyses stratégiques et des évaluations de la menace[30].

[24] Document de travail des services de la Commission : résumé de l'analyse d'impact relative à l'adaptation du cadre juridique de l'Office européen de police au traité de Lisbonne, SWD (2013) 99 final part. 1, Bruxelles, 27 mars 2013 p.3.
[25] Rapport d'information fait au nom de la commission des affaires européennes sur Europol et Eurojust : perspectives d'avenir, n° 477, Sénat sess. ord, 17 avril 2014, p.11.
[26] Règlement Europol, article 3, §1er.
[27] Règlement Europol, article 3, §2.
[28] Règlement Europol, considérant n°6.
[29] Règlement Europol, article 4, §1er.
[30] Règlement Europol, article 4, §§2 et 3.

Au vu des objectifs et des missions de l'Office, il parait évident que le travail engagé par l'agence soit efficace et nécessaire pour les autorités nationales de police. L'analyse criminelle et le recoupement d'informations effectués par Europol, aide les services répressifs nationaux à déterminer si les suspects de leurs enquêtes de police ont déjà retenu l'attention d'autres services répressifs collaborant avec Europol[31].

Chapitre 4 : Structure et gouvernance

L'organisation de l'Office européen de police est régie par le chapitre III du règlement Europol. Sa structure administrative et de gestion se compose principalement d'un conseil d'administration et d'un directeur exécutif[32].

Au sein du conseil d'administration siègent un représentant de chaque État-membre et un représentant de la Commission[33] qui sont sélectionnés, entre autres, pour leurs qualités intellectuelles dans le domaine de la coopération entre services répressifs[34]. Leur mandat a une durée de quatre ans, pouvant être prolongée au besoin[35]. Une des fonctions principales du conseil d'administration est l'adoption annuelle du document contenant la programmation pluriannuelle et le programme de travail annuel de l'agence[36]. La programmation pluriannuelle va globalement exposer la stratégie, les objectifs et les résultats attendus d'Europol. Le programme de travail est, quant à lui, le plan d'activité annuel de l'Office qui va définir ses objectifs et servir de base à la planification budgétaire. Il est utilisé pour communiquer les objectifs de l'agence de manière transparente et structurée[37]. L'adoption du budget annuel d'Europol et de son rapport d'activité annuel consolidé, l'adoption des règles relatives à la prévention et à la gestion des conflits d'intérêts ainsi que celles relatives à la procédure de sélection du directeur exécutif, et la nomination pour certains postes - tels que celui de délégué à la protection des données - font également partie des

[31] Rapport d'information fait au nom de la commission des affaires européennes sur Europol et Eurojust : perspectives d'avenir, n° 477, Sénat sess. ord, 17 avril 2014, p.12.
[32] Règlement Europol, article 9, a) et b).
[33] Règlement Europol, article 10, §1er.
[34] Règlement Europol, article 10, §2.
[35] Règlement Europol, article 10, §4.
[36] Règlement Europol, article 12.
[37] Europol Work Programme 2016, mis en ligne le 3 février 2016, disponible sur https://www.europol.europa.eu/publications-documents/europol-work-programme-2016 (date de la dernière consultation : 12 juin 2020), p.5.

fonctions des membres du conseil d'administration, reprises à l'article 11, paragraphe premier du règlement Europol.

L'Office européen de police est placé sous l'autorité d'un directeur exécutif - nommé par le Conseil - et représentant légalement l'agence. L'article 16 du règlement liste intégralement les fonctions du directeur exécutif dont le poste consiste à mettre en œuvre les missions qui ont été confiées à Europol. Il est chargé d'assurer la gestion de l'agence et exerce ses fonctions en toute indépendance[38]. Le poste est occupé, depuis mai 2018, par la belge Catherine De Bolle qui est secondée par trois directeurs exécutifs adjoints.

Au niveau national, chaque État-membre désigne une unité spéciale de police, considérée comme l'organe de liaison entre les services répressifs nationaux compétents et Europol, chargée de coordonner les relations de coopération avec l'Office[39]. Ces unités nationales assurent la communication de toutes les informations nécessaires à la réalisation des objectifs d'Europol ainsi qu'une communication efficace avec l'agence[40]. Á son tour, Europol est chargé de rédiger annuellement un rapport contenant les informations fournies par chaque État-membre, se basant sur une analyse quantitative et qualitative[41]. Chaque unité nationale désigne au moins un officier de liaison afin de garantir un échange constant d'informations et une coopération effective avec Europol. Les 262 officiers de liaison[42] représentent les intérêts de leur unité nationale auprès de l'agence[43].

Chapitre 5 : Le règlement (UE) 2016/794 du 11 mai 2016 relatif à l'agence de l'Union européenne pour la coopération des services répressifs (Europol)

Section 1 : Objectifs du règlement (UE) 2016/794

Le règlement (UE) 2016/794 du 11 mai 2016 relatif à l'Agence de l'Union européenne pour la coopération des services répressifs, est devenu applicable le 1er mai 2017. Ce sont les articles 87,

[38] Règlement Europol, article 16, §§1, 2 et 4.
[39] Règlement Europol, considérant n°14.
[40] Règlement Europol, article 7, §6, a) et b).
[41] Règlement Europol, article 7, §11.
[42] Europol, *Europol in brief, year of 2019*, mis en ligne le 16 décembre 2020, disponible sur https://www.europol.europa.eu/activities-services/main-reports/europol-in-brief-2019 (date de la dernière consultation : 10 juin 2021), p.3.
[43] Règlement Europol, article 8.

paragraphe 2, point b), et 88 du T.F.U.E. qui constituent les bases juridiques de la règlementation. Le remplacement de la décision 2009/371/JAI par le règlement Europol est justifié par la poursuite de plusieurs objectifs.

Le premier objectif concerne la mise en conformité des textes légaux régissant le fonctionnement d'Europol avec les exigences du traité de Lisbonne. Le règlement a contribué à renforcer la légitimité démocratique de l'agence en instituant un mécanisme de contrôle des activités d'Europol par le Parlement européen, en association avec les parlements nationaux. À l'origine, le Parlement européen n'intervenait que lors de la remise du rapport annuel spécial des activités d'Europol et lors d'éventuelles modifications de la convention portant création à l'Office européen de police[44]. L'entrée en vigueur du règlement s'est accompagnée du renforcement du contrôle démocratique de l'agence par les parlementaires qui jouent dorénavant un rôle actif dans les décisions concernant le budget d'Europol. Ils ont également la capacité de solliciter une audition du président du conseil d'administration, du directeur exécutif ou de leurs remplaçants, pour examiner des questions relatives aux activités d'Europol dans l'accomplissement de ses missions[45].

Le deuxième objectif est le renforcement des capacités de l'agence dans le domaine de la coopération policière, en intensifiant l'échanger de données entre Europol et les États-membres. En effet, afin de respecter les objectifs dictés par le programme de Stockholm et ainsi devenir « le centre névralgique de l'échange d'informations entre les services répressifs des États membres et jouer le rôle de prestataire de services et de plate-forme pour les services répressifs »[46], Europol a mis en place, dans son règlement, des obligations plus strictes incombant aux État-membres et concernant l'alimentation de ses bases de données en informations pertinentes. Avec une base de données plus fournie, Europol est plus à même d'analyser rapidement les formes graves de criminalité transfrontalière et le terrorisme, présents dans l'Union européenne et donc de soutenir plus efficacement les services répressifs nationaux dans leurs enquêtes de police[47].

[44] Rapport d'information fait au nom de la commission des affaires européennes sur Europol et Eurojust : perspectives d'avenir, n° 477, Sénat sess. ord, 17 avril 2014, pp. 14-16.
[45] Règlement Europol, article 51, §2, al. 2, a).
[46] Le programme de Stockholm – une Europe ouverte et sûre qui sert et protège les citoyens, *J.O.U.E.*, C 115/1, 4 mai 2010, point 4.3.1., alinéa 1er.
[47] Proposition de règlement du Parlement européen et du Conseil relatif à l'Agence de l'Union européenne pour la coopération et la formation des services répressifs (Europol) et abrogeant les décisions 2009/371/JAI et 2005/681/JAI, COM (2013) 173 final, Bruxelles, 27 mars 2013, pp. 6-7.

L'amélioration de la gouvernance d'Europol a également motivé la mise en place du règlement. La règlementation a complété les dispositions déjà existantes dans la décision du Conseil et a conformé Europol aux principes gouvernant les agences décentralisées de l'Union européenne afin que le travail du conseil d'administration et du directeur exécutif soit plus efficient[48].

Le règlement Europol a également eu pour conséquence de solidifier le régime de protection des données à caractère personnel, applicable aux activités d'Europol. Le contrôleur européen de la protection des données s'est vu octroyer un rôle primordial de superviseur de la bonne gestion des données personnelles au sein de l'agence et de conseiller d'Europol sur toutes les questions concernant le traitement de données personnelles. En outre, le traitement des données sensibles, comprenant notamment les données des mineurs, des victimes ou des témoins et celles qui révèlent les opinions politiques ou les données médicales de la personne concernée, n'est uniquement possible que dans l'hypothèse où ces données complètent d'autres données à caractère personnel déjà traitées par l'Office[49].

Pour finir, le règlement Europol est directement applicable dans tous les États-membres, y compris l'Irlande qui a expressément demandé de prendre part à l'adoption et à l'application du règlement[50]. Le Royaume-Uni et le Danemark ne participent pas, quant à eux, à l'adoption du règlement et ne sont donc pas soumis à son application[51].

Section 2 : Origine des données

L'Office européen de police est apte à traiter, d'une part, les données à caractère personnel et autres informations qui lui sont fournies par les États-membres, les organes de l'Union européenne, les pays tiers, les organisations internationales et les parties privées et, d'autre part, les données personnelles publiques, en ce compris les informations disponibles sur Internet et au sein des bases de données publiques[52]. Ce sont ces informations qui vont permettre à Europol de remplir ses

[48] *Ibid.*, p. 11.
[49] Rapport d'information fait au nom de la commission des affaires européennes sur Europol et Eurojust : perspectives d'avenir, n° 477, Sénat sess. ord, 17 avril 2014, p. 18 ; règlement Europol, considérant n°43.
[50] Règlement Europol, considérant n°72.
[51] Règlement Europol, considérant n°73 et n°74.
[52] Règlement Europol, article 17.

missions et d'apporter une aide efficace aux États-membres afin de lutter contre les formes graves de criminalité et d'assurer la sécurité des citoyens de l'Union européenne.

Sous-section 1 : Échange des données entre les États membres de l'Union européenne et Europol

À ses début, Europol souffrait véritablement d'un manque d'informations venant des services répressifs nationaux qui étaient réticents à collaborer avec l'agence. En effet, « celui qui détient l'information répugne à la partager, ce qui lui permet de conserver la maîtrise d'une affaire »[53]. Europol qui repose la réussite de ses activités sur la coopération et le partenariat avec les États-membres, avait du mal à pallier le manque de renseignements avec l'accomplissement de ses missions. Aujourd'hui, bien que certaines réticences subsistent toujours dans le partage de données, Europol a réussi à démontrer son indispensabilité dans la coopération pénale européenne et est paradoxalement confronté à un tout autre problème ; celui des méga-données dont nous parlerons longuement dans la suite de ce mémoire.

Europol coopère avec les États-membres de l'Union européenne et traite les informations qui lui sont fournies soit directement par les autorités compétentes des États-membres[54], soit par les unités nationales. Ces unités sont mises en place, au niveau national, afin de servir d'organe de liaison entre l'agence et les autorités compétentes des États-membres[55]. Chaque unité nationale a évidemment accès aux données des services répressifs nationaux afin de coopérer efficacement avec Europol[56]. Notons que tout échange de données entre un État-membre et l'Office européen de police se fait dans le respect du droit national de cet État-membre[57].

Par l'intermédiaire des unités nationales ou des autorités compétentes, les États-membres fournissent à l'agence toutes informations utiles à l'accomplissement de ses objectifs et, par conséquent, toutes informations concernant des formes graves de criminalité. Néanmoins, les

[53] F.-X. ROUX-DEMARE, « L'inaboutissement des mécanismes de coopération opérationnelle » *in Coopération opérationnelle en droit pénal de l'Union européenne* (sous la dir. de C. BILLET et A. TURMO), 1e édition, Bruxelles, Bruylant, 2020, p. 34.
[54] Règlement Europol, article 7, §5.
[55] Règlement Europol, articles 7, §2 et 17, §1er, a).
[56] Règlement Europol, article 7, §3.
[57] Règlement Europol, article 7, §6, d).

États-membres peuvent conserver, en leur sein, toutes informations qui pourraient porter préjudice à leurs intérêts nationaux, jugés comme étant essentiels[58].

Europol reçoit des données directement des États-membres mais en communique également. L'article 22 de la règlementation soulève deux cas de figure. Premièrement, l'agence est dans l'obligation de transmettre à un État-membre toutes informations le concernant. Cependant, Europol doit obtenir préalablement l'autorisation explicite de communiquer ces dernières auprès du fournisseur des informations, s'il s'avère qu'elles sont soumises à des limitations d'accès. Deuxièmement, Europol fournit à un État-membre tous renseignements le concernant qui sont absolument nécessaires à la « prévention d'une menace imminente pour la vie des personnes »[59] et ce, nonobstant toute limitation d'accès. Ce deuxième cas de figure ne libère pas l'agence de son obligation d'avertir parallèlement le fournisseur des informations, du partage des données normalement protégées. Nous entendons par informations soumises à des limitations d'accès, toute information pour laquelle, lors de son transfert à Europol, le fournisseur - que ce soit un État-membre, un organe de l'Union ou un autre partenaire de coopération opérationnelle - a déterminé la finalité de traitement de l'information. En d'autres termes, Europol ne pourra utiliser l'information qu'à des fins pour lesquelles elle lui a été fournie. Tout autre traitement nécessite l'autorisation préalable du fournisseur des informations[60].

En ce qui concerne les données à caractère personnel contenues dans les bases de données d'Europol, elles peuvent directement être transférées à un organe de l'Union européenne, dans le mesure où cela s'avère nécessaire à l'accomplissement de ses missions ou de celles d'Europol[61].

Sous-section 2 : Échange des données entre les parties privées et Europol

En plus de sa coopération avec les États-membres et dans la mesure nécessaire de l'accomplissement de ses missions, Europol coopère avec les partenaires suivants : des organes de l'Union européenne, des autorités de pays tiers, des organisations internationales et des parties

[58] Règlement Europol, article 7, §7.
[59] Règlement Europol, article 22, §2, al. 1er.
[60] Règlement Europol, article 19, §§1 et 2.
[61] Règlement Europol, article 24.

privées[62]. Dans ce chapitre, nous allons analyser la coopération entre Europol et des parties privées. Cette coopération est régie par le chapitre V du règlement Europol.

Le règlement Europol définit la notion de parties privées comme étant « des entités et organismes constitués en vertu du droit d'un État membre ou d'un pays tiers, notamment des entreprises et des sociétés, des associations commerciales, des organisations sans but lucratif et autres personnes morales »,[63] autres que les organisations internationales et les organismes de droit public international. Cette définition inclut donc des sociétés telles que Microsoft, Facebook et Twitter.

L'Office européen de police doit en principe, s'il veut traiter des données à caractère personnel obtenues des parties privées, avoir reçu ces informations par l'intermédiaire d'une unité nationale, d'un point de contact ou d'une autorité d'un pays tiers ou d'une organisation internationale avec lesquelles un accord de coopération a été conclu. Dans l'hypothèse ou Europol reçois des données personnelles directement d'une partie privée, le traitement de ces données ne sera autorisé que dans le but d'identifier l'unité nationale, le point de contact ou l'autorité concernés par ces données. Le but étant de laisser la liberté aux unités nationales, aux points de contact et aux autorités compétentes, de décider s'ils veulent transmettre les données personnelles en question à Europol. Dans l'attente de cette décision, Europol ne peut en aucun cas, traiter les données personnelles reçues directement des parties privées[64]. L'article 26, paragraphe 4 de la règlementation met en lumière un autre scénario ; celui où Europol reçoit des informations d'une partie privée située dans un pays tiers avec lequel Europol n'a conclu aucun accord de coopération. L'agence sera limitée à transmettre ces données uniquement aux États-membres ou aux pays tiers avec lesquels un accord sur la base de l'article 23, la décision 2009/371/JAI ou de l'article 218 du T.F.U.E a été négocié et conclu.

À l'heure actuelle, la capacité d'Europol à échanger des données opérationnelles avec des parties privées, est limitée. Il en découle que certains professionnels du droit estiment que le cadre juridique actuel, régissant la coopération entre l'agence et des parties privées, est insuffisant. En effet, les entités privées sont en possession d'innombrables données et informations pouvant être

[62] Note du Conseil de l'Union européenne, « Europol's cooperation with strategic partners: strengths and possible inefficiencies in cooperation with Private Parties », 10494/19, Bruxelles, 4 juillet 2019, p.1.
[63] Règlement Europol, article 2, f).
[64] Règlement Europol, article 26, §§1 et 2.

utiles et pertinentes pour la réalisation des enquêtes menées par l'Office. Cependant, leur transfert vers les bases de données d'Europol n'est pas toujours permis par le règlement en raison, par exemple, du fait que ces données n'ont pas de destinataire ou de victime spécifique et ne répondent donc pas aux conditions de traitement inscrites dans la règlementation. De plus, le règlement limite Europol dans ses capacités à lutter efficacement contre la criminalité transfrontalière et le terrorisme en ne lui permettant pas de « servir de canal permettant aux parties privées de signaler le retrait proactif de contenus »[65]. Il serait intéressant de permettre à l'agence d'avoir systématiquement accès aux données personnelles relatives à un signalement ou un retrait de contenu terroriste sur Internet. En somme, élargir la coopération entre Europol et des parties privées, en permettant un échange de données à caractère personnel plus souple, favoriserait une détection plus précoce des activités criminelles[66].

Bien qu'il soit fort probable que l'élargissement de la coopération avec des entités privées ait un effet positif sur la prévention de la criminalité transfrontalière, il n'empêche que l'échange d'informations entre Europol et des parties privées touche à la question du respect de certains droits fondamentaux dont le droit à la protection des données à caractère personnel. Sachant que l'Union européenne a pour objectif d'assurer la protection des droits fondamentaux des citoyens européens et notamment de s'assurer que l'échange de données avec des parties privées ne porte pas atteinte à ces droits, il est légitime de se poser des questions quant à de la nécessité du transfert de données à caractère personnel envers des entités privées[67]. « Dans quelle mesure la coopération entre Europol et les parties privées apporte-t-elle une valeur ajoutée au travail de répression tant au niveau de l'UE que des États membres ? »[68] et comment Europol peut-il combiner l'échange et le traitement rapide d'informations avec des parties privées, avec l'assurance que le droit à la protection des données à caractère personnel des citoyens européens sera respecté ?

Au vu de l'évolution rapide des technologies et de l'augmentation des activités criminelles transfrontalières, le Conseil de l'Union européenne considère qu'il y a une nécessité opérationnelle

[65] Note du Conseil de l'Union européenne, « Europol's cooperation with strategic partners: strengths and possible inefficiencies in cooperation with Private Parties », 10494/19, Bruxelles, 4 juillet 2019, p.6. Traduit de l'anglais « *to serve as a channel for private parties to report proactive takedown of content* ».
[66] *Ibid.*, pp. 3-6.
[67] C. BILLET, « Le transfert de données à caractère personnel aux États tiers : l'évolution de la protection par l'UE » *in Droits et souveraineté numérique en Europe* (sous la dir. de A. BLANDIN), 1ère édition, Bruxelles, Bruylant, 2016, p. 166.
[68] Note du Conseil de l'Union européenne, *opcit.*, p. 7.

urgente de permettre à Europol de recevoir des données personnelles directement des entités privées[69]. Certaines dispositions[70] de la règlementation ne permettent pas à l'agence de traiter les informations obtenues auprès des parties privées, sur leur fond, étant donné l'obligation de communiquer ces informations préalablement à une unité nationale, à un point de contact d'un pays tiers ou à une organisation internationale. Cette exigence fait perdre un temps considérable à l'Office européen de police qui a des chances de se retrouver, en fin de compte, avec des données dépassées ou n'ayant plus grand intérêt pour l'enquête. Selon le Conseil, l'agence serait plus efficace dans sa lutte contre les formes graves de criminalité si elle parvenait à collecter et à traiter rapidement les données personnelles obtenues directement des parties privées[71].

Nous sommes conscients que les données à caractère personnel obtenues directement des parties privées sont devenues, au fil des années, des informations à haute valeur ajoutée pour Europol et que cette évolution nécessite une évolution équivalente dans le cadre législatif de l'agence. Nous sommes également conscients de l'importance et de l'utilité pour Europol de traiter des données personnelles recueillies auprès de parties privées, sachant que ces entités sont en possession d'un nombre incalculable d'informations leur permettant de dresser le portrait de n'importe quel citoyen. Il est d'ailleurs courant d'entendre des slogans tels que « Google en sait beaucoup plus sur nous que nous-mêmes ». Il n'empêche qu'il semble difficile de concilier ce recueil massif de données avec une protection adéquate des droits fondamentaux des citoyens européens. Quoi qu'il en soit, ce sujet est en cours de négociations, étant donné que la proposition de règlement du Parlement européen et du Conseil ayant pour objectif de modifier le règlement (UE) 2016/794, aimerait permettre à Europol de coopérer plus efficacement avec les parties privées, tout en garantissant un respect du droit à la protection des données à caractère personnel. Une volonté qui parait belle, voir utopique. Peut-on vraiment concilier les deux ? Nous y reviendrons au cours de ce mémoire.

Section 3 : Base de données

En tant qu'agence facilitant l'échange d'informations entre les États-membres de l'Union européenne, Europol a besoin de bases de données spécifiques pour remplir ses fonctions. La

[69] Conseil de l'Union européenne, Conclusions du Conseil sur la coopération entre Europol et les parties privées, 14745/19, Bruxelles, 2 décembre 2019, p.5.
[70] Notamment les articles 17 et 26 du règlement Europol.
[71] Conseil de l'Union européenne, *opcit.*, pp. 2-3.

décision du Conseil portant création à l'Office européen de police, indiquait que le traitement des informations s'organisait autour de systèmes. Tel est le cas du système d'information Europol (ci-après « S.I.E. »). Ce système d'information est une base de données centralisée, hébergée par Europol, au moyen de laquelle les États-membres et autres partenaires de l'agence, stockent des informations à caractère pénal relevant du mandat d'Europol et effectuent des recherches en la matière[72]. Le S.I.E. contient des données relatives à des personnes impliquées dans des activités criminelles ainsi que des données relatives à des infractions. On y retrouve des information sur des sociétés, des véhicules, des documents d'identité, des numéros de téléphones, des adresses postales, des armes à feu, des empreintes digitales ou encore des échantillons ADN, de telle sorte que tous les éléments de preuve et de renseignement en matière de criminalité grave et de terrorisme soient récoltés et stockés dans la base de données[73].

Il est intriguant de voir que le règlement Europol ne fait aucunement mention d'une quelconque base de données ou d'un système d'information. Cette omission n'est pas anodine ou involontaire, elle témoigne d'une volonté de mettre en place un nouveau concept qui est celui de la gestion intégrée des données (*Integrated Data Management Concept).* La gestion intégrée des données permet de renforcer la capacité de soutien opérationnel d'Europol en lui permettant de déceler des liens entre différentes enquêtes grâce à un recoupement des informations disponibles et d'identifier les tendances nouvelles en matière de criminalité transfrontalière[74]. Néanmoins, afin de ne pas brusquer les utilisateurs, ces derniers peuvent continuer à se servir des bases de données instituées au sein de la décision Europol, jusqu'à ce que les nouvelles mesures soient encrées[75].

Le réseau SIENA, dont il est fait mention une seule fois au sein de la règlementation Europol, est un réseau d'échange sécurisé d'informations destiné à être le canal privilégié de communication

[72] Communication de la Commission au Parlement européen et au Conseil du 6 avril 2016 au sujet des systèmes d'information plus robustes et plus intelligents au service des frontières et de la sécurité, COM (2016) 205 final, Bruxelles, 6 avril 2016, p. 29.
[73] Conseil de l'Union européenne, Manuel sur l'échange d'informations en matière répressive, 5825/20, Bruxelles, 2 décembre 2020, p. 75.
[74] Exposé des motifs du Conseil: Position (UE) no 8/2016 du Conseil en première lecture en vue de l'adoption du règlement du Parlement européen et du Conseil relatif à l'Agence de l'Union européenne pour la coopération des services répressifs (Europol) et remplaçant et abrogeant les décisions 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI et 2009/968/JAI du Conseil, *J.O.U.E.*, C 169/60, 11 mai 2016, p.3.
[75] Conseil de l'Union européenne, Manuel sur l'échange d'informations en matière répressive, 5825/20, Bruxelles, 2 décembre 2020, p. 124.

de données en matière criminelle au sein de l'Union européenne[76]. Il a été mis en place afin d'assurer un échange de données rapide et sécurisé entre Europol, les États-membres, les organes de l'Union européenne, les pays tiers et les organisations internationales. Le réseau SIENA doit garantir un niveau élevé de protection des données à caractère personnel, ce qui implique que, pour chaque donnée SIENA, une indication sur sa confidentialité et sa fiabilité doivent être mentionnées ainsi qu'une indication à propos de la finalité des opérations de traitement[77].

Enfin, le principe de la finalité du traitement est la seule règle qui a été retenue par le règlement Europol au sujet de la protection des données personnelles. En d'autres termes, aucune règle n'indique dans quelle base de données les données à caractère personnel doivent se trouver[78].

Sous-section 1 : Type de données

Vous l'aurez compris, Europol traite les informations mises à sa disposition, y compris des données à caractère personnel, afin d'accomplir ses objectifs. Seulement, le traitement des données à caractère personnel doit répondre à certaines finalités, listées à l'article 18 de la règlementation, pour être autorisé. On y retrouve le traitement dans le but de recouper des informations utiles à établir un lien entre plusieurs affaires criminelles, le traitement avec pour objectif de mener une analyse stratégique, thématique ou opérationnelle ainsi que le traitement permettant de faciliter un échange d'informations. Deux questions sont pertinentes : quelles sont les catégories de données à caractère personnel pouvant être collectées et traitées ? Quelles sont les personnes concernées dont les données à caractère personnel peuvent être collectées et traitées ?

À des fins de recoupement d'informations, Europol est habilité à collecter et à traiter des données relatives au nom, au pseudonyme, au lieu de naissance, de résidence et de profession de la personne concernée, toutes les données figurant sur ses documents officiels ainsi que tout autre élément permettant de l'identifier[79]. En plus de ces données, toutes informations au sujet de condamnations, d'infractions pénales avérées ou présumées de la personne concernée peuvent

[76] Commission européenne, Communication de la Commission au Parlement européen et au Conseil du 6 avril 2016 au sujet des systèmes d'information plus robustes et plus intelligents au service des frontières et de la sécurité, COM (2016) 205 final, Bruxelles, p. 8.
[77] Règlement Europol, considérant n°24.
[78] European Data Protection Supervisor, EDPS Decision on the own initiative inquiry on Europol's big data challenge, C 2019-0370, Bruxelles, 18 septembre 2020, pt. 4.2.
[79] Règlement Europol, annexe II, A., §2.

également être collectées et traitées[80]. Nous entendons par personne concernée toutes « personnes qui, au regard du droit national de l'État membre concerné, sont soupçonnées d'avoir commis une infraction ou participé à une infraction relevant de la compétence d'Europol, ou qui ont été condamnées pour une telle infraction »[81] et de toutes « personnes pour lesquelles il existe des indices concrets ou de bonnes raisons de croire, au regard du droit national de l'État membre concerné, qu'elles commettront des infractions pénales relevant de la compétence d'Europol »[82].

Nous remarquons qu'à des fins d'analyses de nature stratégique, thématique et opérationnelle ou à des fins de facilitation de l'échange d'informations entre Europol et ses collaborateurs, la liste des personnes pouvant faire l'objet d'une collecte et d'un traitement de leurs données personnelles s'allonge notablement. D'une part, les données personnelles « des personnes qui, en application du droit national de l'État membre concerné, sont soupçonnées d'avoir commis une infraction ou participé à une infraction pénale relevant de la compétence d'Europol, ou qui ont été condamnées pour une telle infraction »[83] et « des personnes pour lesquelles il existe des indices concrets ou de bonnes raisons de croire, au regard du droit national de l'État membre concerné, qu'elles commettront des infractions pénales relevant de la compétence d'Europol »[84] sont collectées et traitées. Europol gère les données à caractère personnel des personnes citées ci-dessus, à partir du moment où elles apportent des renseignements sur l'état civil de la personne concernée, sur sa description physique, sa profession et ses qualifications, sur son statut financier, sur son comportement et son mode de vie, sur ses contacts et son entourage, sur les moyens de transport et de communication qu'elle utilise, sur ses antécédents judicaires avérés ou présumés ainsi que sur toutes personnes morales associées[85]. Jusqu'ici, rien de vraiment alarmant, Europol s'attaque à des personnes soupçonnées de commettre ou d'avoir commis une infraction pénale ou condamnées pour une telle infraction.

Par contre, ce qui suscite notre inquiétude est la deuxième partie de la liste. Elle concerne la collecte et le traitement de données personnelles se rapportant à « des personnes qui pourront être appelées à témoigner dans le cadre d'enquêtes portant sur les infractions considérées ou de

[80] Règlement Europol, annexe II, A., §3.
[81] Règlement Europol, annexe II, A., §1er, a).
[82] Règlement Europol, annexe II, A., §1er, b).
[83] Règlement Europol, annexe II, B., §1er, a).
[84] Règlement Europol, annexe II, B., §1er, b).
[85] Règlement Europol, annexe II, B., §2.

poursuites pénales ultérieures »[86] ; à « des personnes qui ont été victimes d'une des infractions considérées ou pour lesquelles il existe certains faits qui permettent de penser qu'elles pourraient être les victimes d'une telle infraction »[87] ; à « des contacts et l'entourage »[88] de toutes les personnes citées-ci-dessus ainsi qu'à « des personnes pouvant fournir des informations sur les infractions pénales considérées »[89]. Si elles sont nécessaires au besoin de l'enquête, les mêmes données que celles qui sont analysées pour des personnes soupçonnées de commettre ou d'avoir commis une infraction pénale ou condamnées pour une telle infraction, sont également collectées et traitées.

Est-il réellement proportionnel, pour le besoin d'une enquête, de collecter et de traiter les données d'autant de personnes lorsqu'on sait que la protection de la vie privée et la protection des données à caractère personnel sont des droits fondamentaux ? Cette question amène à un débat difficile, celui du juste équilibre entre les impératifs de sécurité en Europe et la protection de la vie privée de ses citoyens. Nous tenterons d'apporter des éléments de réponse à ce débat délicat dans la dernière partie de ce mémoire.

Sous-section 2 : Délais de conservation des données à caractère personnel

La règlementation traite des délais de conservation et d'effacement des données personnelles en son article 31. Théoriquement, les données à caractère personnel ne sont conservées par l'agence que pour le temps nécessaire et proportionné à l'accomplissement des finalités pour lesquelles elles ont été collectées. Après trois ans de conservation, Europol décide s'il y a lieu, pour remplir ses missions, de continuer à stocker les données à caractère personnel. Dans l'affirmative, un réexamen à l'issue d'une nouvelle période de trois ans aura lieu.

Les États-membres, les organes de l'Union, les pays tiers et les organisations internationales, peuvent exiger une limitation de conservation des données personnelles qu'ils transfèrent à Europol. Si l'Office juge qu'il est impératif de maintenir le stockage des données et ce, malgré la présence d'une limitation attachée à ces données, il doit en demander l'autorisation auprès du fournisseur des données et justifier sa demande[90].

[86] Règlement Europol, annexe II, B., §1er, c).
[87] Règlement Europol, annexe II, B., §1er, d).
[88] Règlement Europol, annexe II, B., §1er, e).
[89] Règlement Europol, annexe II, B., §1er, f).
[90] Règlement Europol, article 31, §4.

L'effacement de données à caractère personnel qui présentent un risque de nuire aux intérêts d'une personne devant être protégée, ne pourra avoir lieu dans aucun cas. Le même sort est réservé aux données personnelles utiles à l'exercice ou à la défense d'un droit en justice et aux données pour lesquelles la personne concernée renonce à leur effacement[91].

Sous-section 3 : Accès aux données à caractère personnel

Bien qu'il ne soit pas utile, dans le cadre de ce mémoire, d'énumérer toutes les règles d'accès aux données personnelles, il est toutefois intéressant de mentionner les personnes pouvant y accéder.

Conformément à leur droit national, les États-membres ont accès à toutes les données fournies à Europol sans que cet accès ne porte préjudice au droit des autres États-membres, des organes de l'Union, des pays tiers et des organisations internationales[92]. De plus, l'accès aux informations contenues au sein des bases de données hébergées par Europol, est autorisé aux membres du personnel de l'agence dans la mesure nécessaire à l'exécution de leurs fonctions[93].

L'unité de coopération judicaire de l'Union européenne « Eurojust » et l'Office européen de lutte antifraude « OLAF » disposent d'un accès indirect aux données fournies à Europol et ce, sans préjudice de la présence d'une quelconque limitation d'accès ou d'utilisation, formulée par le fournisseur des données[94].

Enfin, toute personne concernée dispose d'un droit d'accès, uniquement au regard des données à caractère personnel la concernant. Pour ce faire, cette dernière doit introduire une demande d'accès auprès de l'autorité compétente de l'État-membre de son choix qui transmettra cette demande à Europol. L'Office aura, quant à lui, le choix d'autoriser, de refuser ou de limiter l'accès demandé, selon une évaluation de la balance entre les mesures de sécurité et les intérêts de la personne concernée. La personne concernée à qui Europol a refusé ou limité l'accès à ses données, pourra introduire une réclamation auprès du C.E.P.D.[95].

[91] Règlement Europol, article 31, §6.
[92] Règlement Europol, article 20, §1er.
[93] Règlement Europol, article 20, §4.
[94] Règlement Europol, article 21.
[95] Règlement Europol, article 36.

PARTIE 2 : LE TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL

Chapitre 1 : Définitions

Pour comprendre l'objet de ce mémoire, il est primordial de définir deux concepts clés : les données à caractère personnel et le traitement de ces données.

Section 1 : Données à caractère personnel

Le droit européen définit une donnée à caractère personnel comme étant « *toute information se rapportant à une personne physique identifiée ou identifiable* »[96]. En d'autres termes, toute information permettant d'identifier une personne physique à part entière et de saisir sa personnalité et son comportement, est considérée comme étant une donnée à caractère personnel. Certains identifiants, tels qu'un nom, un numéro d'identification, une plaque d'immatriculation, des données de localisation, des données de comportement en ligne, une empreinte digitale, un échantillon d'ADN, une adresse mail ou postale ou encore un numéro de téléphone, vont permettre de révéler directement ou indirectement l'identité d'une personne physique[97]. Une donnée à caractère personnel inclut donc toute forme d'information[98].

Une donnée est personnelle à partir du moment où elle permet l'indentification directe, c'est-à-dire qu'elle permet de relier immédiatement une donnée à une personne ou l'identification indirecte d'une personne physique. On parlera d'identification indirecte lorsque une information ne permet pas à elle seule d'identifier une personne concernée mais que la combinaison de cette information

[96] 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 (ci-après le « RGPD »), article 4, 1) ; Convention 108 + du Conseil de l'Europe relatif à la protection des personnes à l'égard du traitement des données à caractère personnel, article 2, a. ; Directive (UE) 2016/680 de 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 (ci-après la « Directive Police »), article 3, 1.

[97] *Ibid.*

[98] C. de TERWANGNE, « Chapitre 9. - Internet et la protection de la vie privée et des données à caractère personnel » *in L'Europe des droits de l'homme à l'heure d'Internet* (sous la dir. de C. de TERWANGNE et Q. Van ENIS), 1e édition, Bruxelles, Bruylant, 2019, p. 328.

avec d'autres données permettent d'identifier la personne physique[99]. L'identification dont il est fait référence « doit se comprendre non comme l'établissement de l'identité civile d'un individu mais comme l'individualisation de cette personne et la capacité de la traiter différemment des autres »[100].

Une étude montre que quatre points spatio-temporels suffisent pour identifier de manière précise nonante pour cent des individus[101]. Une donnée en apparence insignifiante et anodine peut tout à fait mener à l'identification unique d'un individu ce qui rend l'analyse d'une donnée à caractère personnel encore plus difficile.

Selon la jurisprudence de la Cour de justice de l'Union européenne (ci-après « C.J.U.E » ou « Cour de justice ») qui apporte une définition large des données à caractère personnel, toute donnée est une donnée personnelle ou susceptible de le devenir[102]. Par exemple, la Cour de Justice qualifie de données personnelles des informations relatives aux conditions de travail d'une personne physique ou à ses passe-temps[103], une liste de participants à une réunion[104] ou encore une copie d'examen[105]. Elle ajoute que des informations diffusées sur Internet et destinées à un public indéfini en nombre, peuvent également être considérées comme étant des données à caractère personnel[106].

Enfin, le concept de données à caractère personnel est, depuis son origine, uniquement réservé aux personnes physiques. On entend par personnes physiques aussi bien les majeurs, les mineurs que les personnes placées sous un régime de protection judiciaire[107].

Section 2 : Traitement des données à caractère personnel

[99] O. TAMBOU, « Chapitre 1. - Champ d'application matériel du droit européen de la protection des données à caractère personnel » *in Manuel de droit européen de la protection des données à caractère personnel* (sous la dir. de J.-B. AUBY), Bruxelles, Bruylant, 2020, p.60.
[100] C. de TERWANGNE, *opcit.*, p. 329.
[101] Y.-A. de MONTJOYE, L. RADAELLI, V.K. SINGH et A. PENTLAND, « Identity and privacy. Unique in the shopping mall: on the reidentifiability of credit card metadata », *Science*, vol. 347, n° 6221, 2015, p. 536.
[102] O. TAMBOU, *opcit.*, pp. 58-59.
[103] C.J.U.E., arrêt du 6 novembre 2003, *Lindqvist*, aff. C-101/01, EU:C:2003:596, pt. 24.
[104] C.J.U.E., arrête du 26 juin 2010, *Commission européenne c. The Bavarian Lager*, aff. C-28/08, EU:C:2010:378, pt. 70.
[105] C.J.U.E., arrêt du 20 décembre 2017, *Peter Nowak c. Data Protection Commissionner*, aff. C-434/16, EU:C:2017:994, pt. 62.
[106] C.J.U.E., arrêt du 16 décembre 2008, *Tietosuojavaltuutettu c. Satakunnan Markkinapörssi Oy, Satamedia Oy*, aff. C-73/07, EU:C:2008:727, pt. 65.
[107] O. TAMBOU, *opcit.*, p. 62.

Le droit européen désigne le traitement comme étant toute opération sur les données personnelles. En effet, il s'agit de « *toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données 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* »[108]. Cette définition liste, de manière non exhaustive, les différentes opérations qui constituent un traitement. Il existe deux types de traitements de données personnelles ; le traitement automatisé, informatisé, et le traitement non-automatisé des données. Nous entendons par là les fichiers en version papier. La Charte des droits fondamentaux ajoute la nécessité d'un traitement loyal des données personnelles se basant sur le consentement de la personne concernée ou sur un autre fondement légitime prévu par la loi[109].

La Cour européenne des droits de l'Homme considère que la simple conservation de données à caractère personnel, indépendamment de leurs utilisations ultérieures, porte préjudice au droit à la vie privée et familiale de la personnes concernée, institué au sein de l'article 8 de la Convention européenne des droits de l'Homme[110]. La Cour de justice estime, quant à elle, que le traitement de données à caractère personnel constitue une ingérence à la vie privée des individus, droit garanti par l'article 7 de la Charte des droits fondamentaux[111]. Par conséquent et au vu de l'atteinte que le traitement des données personnelles peut avoir sur les droits fondamentaux, les deux juridictions estiment que le traitement de données personnelles par Europol, dans le cadre de mesures de surveillance, doit être strictement nécessaire pour être compatible avec notre société démocratique[112].

---

[108] RGPD, article 4, 2) ; Directive Police, article 3, 2) ; Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) n° 45/2001 et la décision n° 1247/2002/CE, article 3, 3).

[109] Charte des droits fondamentaux de l'Union européenne, article 8, 2).

[110] C.E.D.H., arrêt du 4 décembre 2008, *S. et Marper c. Royaume-Uni*, requêtes 30562/04 et 30566/04, §67.

[111] C.J.U.E., arrêt du 16 juillet 2020, *Data Protection Commissioner c. Facebook Ireland Limited et Maximillian Schrems*, aff. C-311/18, ECLI:EU:C:2020:559, §170.

[112] CCBE, Position du CCBE sur la proposition de règlement modifiant le règlement (UE) 2016/794 en ce qui concerne la coopération d'Europol avec les parties privées, le traitement de données à caractère personnel par Europol à l'appui d'enquêtes pénales et le rôle d'Europol en matière de recherche et d'innovation, 6 mai 2021, p.2.

Chapitre 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 (règlement général sur la protection des données)

Section 1 : Objectif du RGPD

Le règlement général sur la protection des données qui, comme son nom l'indique, a pour objectifs d'améliorer la protection des données et de faciliter la libre circulation des données à caractère personnel sur le marché unique, actualise la directive 95/46/CE[113] et la Convention 108 du Conseil de l'Europe[114]. Les nonante-neuf articles du règlement expriment une volonté de mettre en place un modèle européen uniformisé et cohérent de la protection des données afin d'assurer un même niveau de protection pour les personnes physiques, ainsi qu'une effectivité de leurs droits, tout en soumettant les responsables du traitement des données à un même niveau d'obligation et de responsabilité[115].

Le champ d'application matériel du règlement européen s'applique à l'ensemble des traitements de données à caractère personnel, qu'ils soient automatisés ou non automatisés[116]. Le champ d'application territorial du RGPD est défini, quant à lui, sur base de trois critères distincts repris à l'article 3 dudit règlement. Le champ d'application territorial s'étend bien au-delà des frontières européennes, étant donné qu'il est uniquement requis qu'un traitement - qu'il soit établi dans l'Union européenne ou non - implique les données d'un résident européen pour que le règlement soit applicable. De surcroît, sont également prises en compte les situations dans lesquelles un responsable de traitement, non établis dans l'Union européenne, serait tout de même soumis au

[113] Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, *J.O.C.E.*, L 281, 23 novembre 1995.
[114] Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, *STE*, n° 108, 28 janvier 1981.
[115] Y. POULLET, « Avant-propos. Le RGPD – une volonté de bien faire : certes ! … mais appropriée ? » *in Le règlement général sur la protection des données (RGPD/GDPR)* (sous la dir. de C. DE TERWANGNE et K. ROSIER), 1ère édition, Bruxelles, Larcier, 2018, p. 8-9.
[116] RGPD, article 2, §1er.

RGPD en raison du droit international public[117]. C'est notamment le cas des représentants diplomatiques ou consulaires d'un État-membre[118].

Le RGPD propose une version modernisée de la protection des données à caractère personnel. Cette réglementation tend à s'adapter aux nouveaux phénomènes technologiques, intervenus depuis 1995, tels que le phénomène du *Big Data* et l'émergence de l'intelligence artificielle qui modifient considérablement la façon de collecter, de stocker et de traiter des données personnelles[119]. Nous aborderons ces sujets dans la dernière partie de ce mémoire.

La notion de cohérence revient à de nombreuses reprises au sein du RGPD, sans jamais être réellement définie. La mise en cohérence de la protection des données à caractère personnel est une promesse du règlement européen. D'ailleurs, ce sont les objectifs de cohérence qui ont motivé l'utilisation d'un règlement à la place d'une directive étant donné que cet instrument juridique est, par nature, directement applicable dans l'ordre juridique des États-membres. Cependant, le RGPD est considéré comme un règlement hybride, en ce sens qu'il a été contraint de conserver de multiples marges de manœuvre qui imposent des adaptations au niveau national. Il existe, encore aujourd'hui, des règlementations spécifiques dans les États-membres qui dérogent au RGPD. L'idée principale derrière la mise en place de cette règlementation européenne, est l'application homogène de la protection des données à caractère personnel au sein des États-membres[120].

Des précisions nouvelles sont apportées au RGPD, notamment sur le consentement de la personne concernée vis-à-vis du traitement de ses données personnelles. Selon le rapporteur du Parlement européen, « le consentement devrait demeurer l'élément clé de l'approche de la protection des données de l'Union européenne, puisqu'il s'agit du meilleur moyen pour que les personnes puissent contrôler les activités de traitement des données »[121]. La directive 95/46/CE exigeait un consentement « indubitable » et, pour le traitement des données sensibles, un

[117] RGPD, article 3, §3.
[118] RGPD, considérant n°25.
[119] Y. POULLET, *opcit.*, p. 10.
[120] Colloque du 20 janvier 2020 organisé par le CEDAG (Centre de Droit des Affaires et de Gestion de la Faculté de Droit, d'économie et de gestion de l'Université de Paris), *Le droit européen des données personnelles : à la recherche d'une cohérence (1ère partie)*, disponible sur : https://www.youtube.com/watch?v=kmdzeLkPCNA (date de la dernière consultation : 30 juin 2021).
[121] Rapport sur la proposition de règlement sur la proposition de règlement du Parlement européen et du Conseil 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 (règlement général sur la protection des données), COM(2012)0011, C7-0025/2012, 21 novembre 2013, pp. 223-224.

consentement « explicite », tandis que la règlementation européenne, dans l'optique de renforcer la qualité du consentement, requiert un consentement « univoque » pour lequel une déclaration ou un acte positif clair devront être donné[122]. Par exemple, le consentement peut être donné par voie électronique, en cochant une case sur un site Internet, ou par une quelconque déclaration écrite. En revanche, aucun consentement de la personne concernée ne peut être déduit de son silence, les consentements tacites ou passifs sont donc exclus[123]. L'objectif poursuivi est de s'assurer que la personne concernée ait bel et bien donné son consentement libre, éclairé et spécifique pour le traitement de ses données[124]. En vertu du règlement européen, la personne concernée peut retirer son consentement à tout moment, aussi aisément qu'elle l'a donné et sans que ce retrait ne lui occasionne un quelconque préjudice[125]. Notons que « le retrait du consentement ne compromet pas la licéité du traitement fondé sur le consentement effectué avant ce retrait »[126].

D'autres articles font apparaitre des situations nouvelles, c'est le cas de l'article 11 qui vise des situations pour lesquelles les traitements de données ne nécessitent pas l'identification des personnes concernées. Cette disposition spécifie que dans les cas où les données à caractère personnel traitées ne suffisent pas à identifier une personne, le responsable du traitement n'est pas dans l'obligation d'obtenir des informations supplémentaires sur la personne concernée dans l'unique but de respecter le règlement européen[127]. Dès lors, la personne physique pour laquelle l'identification est impossible ne se verra pas accorder les droits, tels que le droit d'accès ou le droit de rectification, dont il est question dans le RGPD. Enfin, il est important de noter qu'il incombe au responsable du traitement d'apporter la preuve qu'il était dans l'impossibilité d'identifier la personne concernée[128].

Conformément à l'article 97 du RGPD, la Commission européenne a présenté au Parlement européen et au Conseil, le 24 juin 2020, son premier rapport d''évaluation et de réexamen du règlement général de la protection des données. D'après le constat général, la Commission est

---

[122] A. MICHEL, « Le traçage comportemental des internautes sur les réseaux sociaux : l'affaire des « cookies Facebook », véritable saga judiciaire ? », *R.D.T.I.*, 2019/1, p.86.
[123] RGPD, considérant n°32.
[124] C. de TERWANGNE, « Chapitre 2. - Hypothèses de licéité des traitements » *in Le règlement général sur la protection des données (RGPD/GDPR)* (sous la dir. de C. DE TERWANGNE et K. ROSIER), 1ére édition, Bruxelles, Larcier, 2018, p. 125.
[125] RGPD, considérant n°42.
[126] RGPD, article 7, §3.
[127] RGPD, considérant n°57.
[128] A. BENSOUSSAN, « Chapitre 2. - Principes » *in Règlement européen sur la protection des données* (sous la dir. de A. BENSOUSSAN), 2e édition, Bruxelles, Bruylant, 2017, pp. 320-321.

positivement étonnée de l'impact que le RGPD a eu sur les droits des citoyens - désormais mieux armés et plus conscients de leurs droits - et met en avant le succès avec lequel le règlement européen a atteint ses objectifs[129]. La Commission ajoute que le RGPD a su démontrer son importance dans l'élaboration de solutions numériques dans des situations imprévues telle que la crise sanitaire encore d'actualité aujourd'hui. Seulement deux ans après son entrée en application, le RGPD est devenu une référence mondiale en matière de protection de données à caractère personnel et joue un vrai rôle de guide dans ce domaine. Néanmoins, certains points doivent être améliorés notamment afin de s'aligner avec les transitions numériques. De plus, un travail majeur doit encore être entrepris afin de garantir l'harmonisation dans l'application de cette réglementation hybride.

Section 2 : Europol face au RGPD

En dépit du fait que le règlement général sur la protection des données ne s'applique pas à l'Office européen de police, il exerce une influence importante sur ses activités. Dans son rapport d'évaluation sur la menace liée à la criminalité organisée sur Internet de 2018, Europol met en lumière certains développements législatifs clés dont le règlement général sur la protection des données. L'agence prend directement un ton critique en expliquant que, bien que cette évolution législative soit positive, elle représente un défi commun pour les services répressifs de l'Union européenne : celui de la perte de données. Par conséquent, le RGPD a un impact sur l'efficacité des activités de l'Office en matière de cybercriminalité[130].

Cette règlementation requiert le signalement de données personnelles dans les 72 heures de la survenance de leur violation. L'entreprise ne respectant pas le RGPD encourt une amende de 20 millions d'euros ou de 4 % de son chiffre d'affaires annuel, le montant le plus élevé étant retenu. Cette exigence a pour conséquence l'augmentation et le financement des piratages informatiques. En effet, depuis l'entrée en vigueur du RGPD, de nombreux hackers piratent les systèmes informatiques des entreprises et demandent une rançon, sous peine de la divulgation des données personnelles des utilisateurs des entreprises. Dans de nombreux cas, les entreprises préfèrent payer une rançon plutôt que les amandes substantielles qu'elles devraient normalement payer aux

[129] Commission européenne, Rapport de la Commission: les règles de l'UE en matière de protection des données donnent aux citoyens les moyens d'agir et sont adaptées à l'ère du numérique, Bruxelles, 24 juin 2020, p.2.
[130] Europol, *Internet Organised Crime Threat Assessment (IOCTA)*, mis en ligne le 18 septembre 2018, disponible sur https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018 (date de la dernière consultation : 3 juillet 2020), p.4.

Autorités de protection des données, pour atteinte à la sécurité des données personnelles de leurs clients[131].

Concernant les enquêtes menées par Europol et par les services de police sur la cybercriminalité, l'une des conséquences les plus impactantes de la mise en place du règlement se rapporte à la base de données WHOIS, considérée comme étant non conforme au RGPD. Le service de recherche WHOIS alimenté par les registres Internet, permet d'obtenir des renseignements sur une adresse IP ou un nom de domaine. L'entrée en vigueur du RGPD a eu pour effet de supprimer toutes les données à caractère personnel, accessibles au public, du service de recherche WHOIS, ce qui a considérablement impacté l'efficacité des enquêtes de police sur la criminalité en ligne. Europol et les services répressifs nationaux, doivent dorénavant engager une procédure administrative afin d'obtenir l'autorisation d'accéder aux informations, anciennement contenues au sein de la base de données WHOIS. Ces procédures formelles nécessitent de longs délais, généralement plus importants que la période de conservation des données demandées, ayant pour conséquence possible qu'au moment où l'accès est autorisé, les données en question n'existent plus. D'une part, la suppression des données personnelles au sein des registres WHOIS ralentit les enquêtes policières et, d'autre part, elle porte préjudice à la confidentialité des enquêtes. En effet, aucune garantie ne permet d'assurer que les opérateurs de registres ou de bureaux d'enregistrement n'avertiront pas leurs clients que leur domaine fait l'objet d'une enquête[132].

Par conséquent, le règlement général sur la protection des données participe indirectement à une réduction de la capacité des services répressifs européens et d'Europol, à enquêter sur la cybercriminalité. Nous remarquons qu'il y a des situations dans lesquelles le renforcement des droits fondamentaux des citoyens, mène à une diminution de l'efficacité des enquêtes criminelles et porte indirectement atteinte à la sécurité. Le RGPD est un exemple du dilemme du *Zero-Sum*, mettant en lumière la lutte constante entre le besoin d'augmenter le droit à la protection des données personnelles sans pour autant porter préjudice à la sécurité en Europe. Nous analyserons ce dilemme dans la partie dédiée aux défis que représentent les méga-données pour Europol.

[131] *Ibid.*, p.28.
[132] Europol, *Internet Organised Crime Threat Assessment (IOCTA)*, mis en ligne le 18 septembre 2018, disponible sur https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018 (date de la dernière consultation : 3 juillet 2020), p. 60.

PARTIE 3 : EUROPOL FACE AU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL

Chapitre 1 : Europol face au défi des méga-données (*Big data*)

Ces dernières décennies, notre monde est entré dans une nouvelle ère : l'ère numérique qui, par des évolutions technologiques, a révolutionné nos sociétés et notre façon de concevoir l'information. Avec l'émergence de cette révolution numérique, est également apparu le concept de « *Big data* » ou de « méga-données » en français[133]. Ce phénomène se fonde sur un principe en vertu duquel au plus il y a de données collectées, mises en commun et analysées, au plus les résultats obtenus seront justes et précis[134] ainsi que pertinents, par rapport aux objectifs poursuivis[135]. La notion de *Big data* est dès lors utilisée lorsqu'on se réfère à un ensemble de données - qu'elles soient à caractère personnel ou non - qui en raison de leur volume ou de leur nature, sont difficilement traitable à l'aide d'une base de données standard. En effet, le traitement du *Big data* nécessite l'utilisation d'outils de stockage spécifiques[136].

De par l'utilisation accrue qu'ont les secteurs privés et publics des méga-données, ce phénomène est rapidement devenu un sujet de discussion important dans les domaines de l'application de la loi et de la sécurité nationale[137]. Une des raisons pour lesquelles les méga-données font autant parler d'elles, est que le traitement d'une large quantité de données peut poser de véritables challenges à la protection des données à caractère personnel et au droit à la vie privée des citoyens, deux droits qui ont été élevés au rang de droits de l'Homme [138].

Bien que les méga-données constituent un défi pour Europol, leur utilisation est aujourd'hui souhaitée par les États-membres et les institutions européennes puisqu'ils sont favorables à

[133] D. DREWER et V. MILADINOVA, « The BIG DATA Challenge: Impact and opportunity of large quantities of information under the Europol Regulation », *Computer Law & Security Review*, vol. 33, 2017, p. 299.
[134] A. DELFORGE, « Comment (ré)concilier RGPD et big data ? », *R.D.T.I.*, 2018/1, p. 28.
[135] P. DELORT, Big Data, Paris, PUF, 2015, p. 6.
[136] European Data Protection Supervisor, EDPS Decision on the own initiative inquiry on Europol's big data challenge, C 2019-0370, Bruxelles, 18 septembre 2020, pt. 1.1.
[137] D. DREWER et V. MILADINOVA, *opcit.*
[138] C. de TERWANGNE, « Chapitre 9. - Internet et la protection de la vie privée et des données à caractère personnel » *in L'Europe des droits de l'homme à l'heure d'Internet* (sous la dir. de C. de TERWANGNE et Q. Van ENIS), 1e édition, Bruxelles, Bruylant, 2019, p. 325-368.

l'intensification de l'échange d'informations et à la création de nouveaux moyens techniques permettant d'augmenter l'efficacité de ces échanges. Ralentir l'essor du phénomène d'amplification et d'accélération du processus de collecte et d'échange de données à caractère personnel, n'est pas désirable ni désiré pour l'efficacité de la coopération policière. Au contraire, nous allons vers un accompagnement de ce phénomène du *Big data*, en comblant toutes les lacunes freinant son essor et en investissant dans des systèmes intelligents de collecte et d'échange d'informations[139].

Section 1 : Émergence du phénomène du *Big data* au sein d'Europol

Depuis quelques années, l'Office européen de police est confronté à un nouveau challenge, celui de la gestion des méga-données. En effet, à ses débuts Europol devait pallier avec un manque crucial de données. Les services répressifs nationaux souhaitant, d'une part, préserver la souveraineté des États membres[140] et, d'autre part, n'étant pas convaincus de l'efficacité et de la nécessité de l'Office, étaient réticents à alimenter ses bases de données. Cette insuffisance a eu des conséquences néfastes sur l'agence qui ne parvenait pas à remplir efficacement ses missions[141]. Par la suite, Europol a surmonté le manque d'alimentation de ses bases de données en menant une campagne de sensibilisation auprès des services répressifs nationaux et en renforçant ses capacités analytiques[142]. Aujourd'hui, la tendance s'est inversée et l'utilisation de *Big data* au sein d'Europol est devenue la norme.

La question de l'émergence du phénomène du *Big data*, compris au sens de l'amplification et de l'accélération du processus de collecte, de traitement et d'échange de données à l'échelon transnational, est avant tout liée à la révolution digitale et aux progrès technologiques et techniques qui se traduisent par une hausse des capacités d'analyse de données à caractère personnel. Ce phénomène s'explique également par l'envie des États-membres de créer une Europe plus sûre et par la nécessité opérationnelle de mettre en place une coopération policière européenne efficace[143].

---

[139] P. BERTHELET, « Europol face au défi des « méga-données » - L'évolution tendancielle d'une coopération policière européenne « guidée par le renseignement » », *R.D.U.E.*, 2019/2, p. 187.
[140] F.-X. ROUX-DEMARE, « L'inaboutissement des mécanismes de coopération opérationnelle » *in Coopération opérationnelle en droit pénal de l'Union européenne* (sous la dir. de C. BILLET et A. TURMO), 1e édition, Bruxelles, Bruylant, 2020, p. 38.
[141] *Ibid.*, p. 160.
[142] P. BERTHELET, *opcit.*, p. 159.
[143] A. TÜRK et P. PIAZZA, « La difficile quête d'un équilibre entre impératifs de sécurité publique et protection de la vie privée », *Cultures & Conflits*, n°76, 2009, pp. 115-116.

Il faut être conscient qu'au sein de la police, l'information a toujours été essentielle pour résoudre des enquêtes. En effet, l'information est considérée comme la base et le moteur des services de police[144].

L'amplification et l'accélération du processus de collecte et d'échange de données sont également dus au fait que les États-membres envoient des volumes de données plus importants à Europol. Les services de police des États-membres se sont dotés de nouveaux moyens technologiques, leur permettant de récolter un nombre incalculable d'informations. Nous retrouvons des technologies telles que les caméras ANPR (*Automatic Number Plate Recognition*) qui, pour des raisons de sécurité, filment en temps réel et prennent une photo de chaque plaque d'immatriculation passant à proximité de la caméra. Ainsi, la police nationale est en mesure de contrôler chaque voiture qui entre et qui sort d'une zone déterminée et de retracer son itinéraire précis. Une technologie similaire est utilisée pour les données de géolocalisation des téléphones portables. La police place des antennes au-dessus des bâtiments afin d'analyser les données de localisation de toutes les personnes étant passées aux alentours de cette antenne[145]. Par conséquent, Europol a été contraint de développer des techniques de *Big data* afin d'analyser ces volumes massifs de données reçues par les États-membres.

Le Contrôleur européen de la protection des données (ci-après le « CEPD ») a également tenté d'identifier les raisons pour lesquelles Europol est confronté au phénomène des *Big data*. Selon lui, trois scénarios justifient le traitement de grands ensembles de données par l'Office européen de police. Premièrement, Europol traite des méga-données lorsqu'il collecte un volume massif d'informations liées à un suspect identifié ou identifiable. Toutes les données collectées et traitées se rapportent à la cible en question, bien qu'il soit possible que les données personnelles d'un individu n'ayant aucun lien avec l'activité criminelle faisant l'objet de l'enquête, soient également collectées et traitées[146]. Le deuxième scénario qui explique pourquoi Europol est confronté au phénomène des *Big data*, concerne la collecte et le traitement massif de données personnelles d'individus n'ayant absolument aucun lien avec une quelconque activité criminelle. C'est par exemple le cas lorsque l'agence collecte des données liées à des activités criminelles distinctes mais qui pourraient être connectées, afin de tenter d'identifier des personnes potentiellement

[144] Entretien avec Pieter-Jan De Grave, Data Protection Officer de la police fédérale belge, annexe I.
[145] Entretien avec Pieter-Jan De Grave, Data Protection Officer de la police fédérale belge, annexe I.
[146] European Data Protection Supervisor, *opcit.*, pt. 3.14.

suspectes[147]. Concrètement, Europol va analyser les données de centaines, voire de milliers, de personnes non pertinentes avec son enquête, pour potentiellement parvenir à cibler les données d'un ou deux individus impliqués dans une activité criminelle. Nous pouvons faire un parallèle avec les technologies utilisées par les services répressifs européens, pour une ou deux plaques d'immatriculation qui vont potentiellement intéresser les enquêteurs, les caméras ANPR vont collecter les données de milliers de voitures appartenant à des personnes n'ayant strictement rien à voir avec l'enquête criminelle en cours[148]. Dans la troisième et dernière situation, nous retrouvons un mélange du premier et du deuxième scénario afin qu'Europol puisse s'impliquer totalement, du début à la fin, dans une enquête criminelle transfrontalière[149].

Section 1 : Promesses du *Big data*

L'utilisation du *Big data* dans le domaine de la sécurité, présente de nombreux avantages potentiels et réalisables. Europol est en possession de larges volumes de données pouvant être exploitées afin de contribuer positivement à l'amélioration de la coopération policière[150].

Premièrement, le *Big data* contribue à une augmentation de l'efficacité opérationnelle des services de police. En effet, le traitement d'un grand volume de données mène à des analyses plus précises des risques, permettant d'effectuer des contrôles plus ciblés. Par conséquent, les services de police augmentent leur efficacité en déployant des ressources, telles que des unités mobiles, des drones policiers ou des hélicoptères de police, là où c'est nécessaire. De plus, grâces aux techniques de *Big data*, des analyses qui autrefois prenaient des semaines ou des mois à être résolues, peuvent aujourd'hui être réalisées en quelques heures seulement[151].

Deuxièmement, l'exploitation de données bénéficie à la reconstitution chronologique d'actes criminels. Les bases de données contenant toujours plus d'informations, permettent en effet, de retracer l'itinéraire précis d'un suspect, de savoir quels appels téléphoniques il a passés et quelles transactions financières il a effectuées. Par exemple, dans certaines enquêtes médiatisées, les

[147] *Ibid.*, pt. 3.15.
[148] Entretien avec Pieter-Jan De Grave, Data Protection Officer de la police fédérale belge, annexe I.
[149] European Data Protection Supervisor, *opcit.*, pt. 3.16.
[150] D. BROEDERS, E. SCHRIJVERS, B. van der SLOOT, R. van BRAKEL, J. de HOOG et E. HIRSCH BALLIN, « Big Data and security policies: Towards a framework for regulating the phases of analytics and use of Big Data », *Computer Law & Security Review*, vol. 33, 2017, pp. 313-314.
[151] WRR, « Big Data in een vrije en veilige samenleving », *Amsterdam University Press*, 2016, p. 76.

enquêteurs belges ont réussi à retrouver les individus suspects, grâce aux caméras ANPR ayant retracé le trajet exact de leur voiture[152]. À l'époque, les enquêteurs procédaient déjà à des reconstitutions historiques des activités criminelles mais avec des données beaucoup moins complètes et plus difficiles d'accès. Aujourd'hui, les technologies utilisant du *Big data* bénéficient aux services de polices en améliorant la qualité des analyses criminelles et la disponibilité des informations, le tout à moindre coût.

L'analyse des activités criminelles en temps réel est également devenue possible, grâce aux évolutions technologiques utilisant du *Big data*. Les services répressifs peuvent désormais suivre des individus, des évènements, des animaux domestiques et des objets, en temps réel. Les caméras placées dans de nombreux endroits, les antennes de géolocalisation, les payements par carte et les réseaux sociaux, sont autant de moyens utilisés par Europol et les services de polices nationaux, pour identifier automatiquement des personnes. Par exemple, les données de localisation de téléphones portables sont utilisées pour estimer le nombre de personnes présentes lors d'un évènement ou d'une manifestation[153]. La police peut donc déployer les ressources nécessaires afin de contrôler ces foules. Il en est de même pour les activités criminelles. Lors d'attaques à main armée, c'est grâce aux données de localisation que les policiers sont en mesure d'estimer le nombre de personnes présentes sur les lieux.

Enfin, la prévision de la criminalité est l'attente principale qu'ont les services de police du fait de la mise en œuvre de techniques de prévision et d'analyse de collecte de données. Le développement de systèmes d'intelligence artificielle permettra de mieux anticiper le moment et le lieu de survenance d'une activité criminelle, d'identifier les futurs délinquants et les futures victimes et de développer des profils « types » de criminels. La création de profils « types » de délinquants se basera sur la probabilité qu'une personne, présentant certaines caractéristiques, commette un acte répréhensible. Par ailleurs, l'identification des auteurs potentiels et des victimes en devenir est certainement la tâche la plus difficile à réaliser. Les masses de données pourront être utilisées pour surveiller des personnes présentant un comportement dit « à risque ». En effet, lorsqu'il est évident qu'un certain comportement entraîne un risque accru de criminalité, des

[152] Entretien avec Pieter-Jan De Grave, Data Protection Officer de la police fédérale belge, annexe I.
[153] WRR, « Big Data in een vrije en veilige samenleving », *Amsterdam University Press*, 2016, p. 78.

mesures préventives peuvent être prises[154]. Notons tout de même que dans la pratique, l'application de systèmes d'intelligence artificielle est encore essentiellement une question d'avenir.

Par conséquent, prévenir la survenance d'activités criminelles plutôt que de devoir appréhender les coupables après que cette activité ait eu lieu, est évidemment très attrayant. La police prédictive ne sera toutefois possible qu'avec la combinaison de l'analyse d'un immense volume de données, en temps réel, avec des informations suffisantes sur les comportements criminels existants[155].

Dans l'ensemble, l'utilisation de *Big data* à des fins de sécurité, contribue à l'augmentation de l'efficacité des enquêtes policières et constitue une innovation majeure dans la lutte de la criminalité. Au vu des avantages que présente le traitement massif de données, il n'est pas difficile de conclure que le Big Data augmente les chances, d'anticiper les actes criminels.

Section 2 : Dangers du *Big data*

Nous avons détecté trois problèmes majeurs à la collecte et au traitement massif de données personnelles opérés par Europol.

Premièrement, l'utilisation du *Big data* au sein d'Europol pose un problème structurel dès lors qu'il se rapporte aux méthodes de travail fondamentales d'Europol. Le Contrôleur européen de la protection des données, chargé de contrôler la licéité des traitements de données personnelles effectués par Europol[156], a ouvert une enquête le 30 avril 2019. Ceci afin de vérifier si l'utilisation du *Big data* par Europol était conforme « avec le cadre de protection des données d'Europol, en particulier avec les principes de limitation de la finalité, de minimisation des données, d'exactitude des données, de limitation du stockage, avec l'impact des violations potentielles de données, de localisation du stockage, de gestion générale et de sécurité des informations »[157]. Le CEPD a démontré qu'au vu de la masse importante de données reçues par Europol, il n'était techniquement pas possible pour l'Office de garantir que toutes les informations contenues dans ces vastes ensembles de données soient conformes à ces limitations. En effet, dans la majorité des situations,

[154] *Ibid.*, p. 80.
[155] WRR, « Big Data in een vrije en veilige samenleving », *Amsterdam University Press*, 2016, p. 80.
[156] Règlement Europol, considérant n°50.
[157] European Data Protection Supervisor, *opcit.*, pt. 2.3. Traduit de l'anglais « *with the Europol's data protection framework, in particular with the principles of purpose limitation, data minimisation, data accuracy, storage limitation, with the impact of potential data breaches, location of storage, general management and information security* ».

le contenu des données collectées par Europol est inconnu jusqu'au moment où l'analyse est menée. Le problème survient lorsque cette masse de données, appartenant à des personnes ne se trouvant pas dans la liste de l'annexe II B du règlement Europol, est stockée au sein des serveurs d'Europol pendant plusieurs années. L'Office stocke cet ensemble de données pour des raisons de véracité, de fiabilité et de traçabilité du processus de renseignements criminels, indépendamment du fait qu'il ait ciblé, dans le fichier, les données de la personne pertinente à son enquête[158]. Il faut se rendre compte que le fait même d'avoir des données à caractère personnel contenues au sein d'une base de données répressive de l'Union européenne, peut potentiellement causer du tort aux personnes concernées. En effet, les personnes concernées qui, nous le rappelons, n'ont généralement aucun lien avec une quelconque enquête de police, risquent d'être liées à tort à une activité criminelle au sein de toute l'Union européenne, engendrant des conséquences dommageables à leur vie privée, professionnelle et familiale ainsi qu'à leur libre circulation. En conclusion, et face au risque que représente le traitement de *Big data* pour les citoyens européens, le CEPD estime que le traitement de grands ensembles de données par Europol n'est pas conforme au principe de minimisation des données, à certains aspects de la finalité des activités de traitement d'informations ainsi qu'à l'annexe II B du règlement Europol. Annexe qui concerne les catégories de données à caractère personnel pouvant être collectées et traitées et les catégories de personnes concernées dont les données peuvent être collectées et traitées[159].

Pieter-Jan De Grave, l'officier en charge de la protection des données au sein de la police fédérale belge que nous avons interrogé, rejoint l'avis du CEPD. Il estime qu'un des problèmes majeurs rencontré par l'utilisation des méga-données est lié au principe général de la minimisation des données. Ce principe veut que la collecte de données à caractère personnel soit adéquate, pertinente et strictement limitée à ce qui est nécessaire au regard des finalités de traitement[160]. Dès lors, l'idée même de celui qui collecte moins, collecte mieux s'avère difficilement conciliable avec la définition du *Big data*. Notons qu'en vertu de l'article 28, paragraphe 4, du règlement Europol, l'Office est responsable du respect du principe de minimisation des données pour toutes données à caractère personnel qu'il traite.

[158] European Data Protection Supervisor, *opcit.*, pt. 4.7 et 4.8.
[159] European Data Protection Supervisor, *opcit.*, pt. 4.10 et 4.11.
[160] RGPD, article 5, §1er, c).

Deuxièmement, la multiplication des informations contenues au sein des bases de données d'Europol augmente évidement les risques d'erreurs ou de dysfonctionnement lors de la collecte, du traitement et de l'échange des informations. Malheureusement, il survient parfois que des citoyens totalement innocents pâtissent de ces erreurs, ce qui peut avoir de graves conséquences sur leurs droits fondamentaux. Sans compter que ces erreurs peuvent également intervenir au détriment de l'efficacité des enquêtes menées par Europol. Une grave erreur est d'ailleurs survenue en 2016, avec une fuite de fichiers d'Europol contenant des données massives concernant des activités terroristes, dont des informations au sujet des attentats de Madrid survenus en 2004. Ces fichiers contenaient des centaines de données à caractère personnel relatives à certaines personnes suspectées, telles que leur nom, prénom et leur numéro de téléphone. Suite à cette fuite, le porte-parole d'Europol, Gerald Hesztera, a reconnu que ces documents secrets avaient été mis en ligne sur Internet suite à une erreur humaine. Cet évènement démontre l'impossibilité technique de garantir la sécurité des données personnelles, toujours plus nombreuses et volumineuses. La collecte et le traitement massifs de données méritent un débat sociétal à partir du moment où une telle fuite de données provoque une atteinte extrême aux droits à la vie privée et à la protection des données à caractère personnel ainsi qu'une ingérence au doit à la présomption d'innocence des personnes concernées[161].

En lien avec ce deuxième problème, nous pouvons ajouter un danger supplémentaire lié à la collecte et au stockage de données massives ; le danger des hackings et des piratages informatiques. À l'heure actuelle, la masse de données collectée par Europol est entre de bonnes mains soit entre les mains d'un service de police européen luttant contre les formes grave de criminalité et de terrorisme. Cependant si les serveurs d'Europol se font pirater et que ces données se retrouvent entre de mauvaises mains, cela pourrait avoir des conséquences désastreuses[162]. Par conséquent, il incombe à Europol de garantir une protection parfaite de ses bases de données.

Concernant les problèmes cités ci-dessus, le CEPD estime que l'Office européen de police est le mieux placé pour trouver des solutions appropriées afin d'atténuer les risques que ces activés de

[161] AEDH, *Europol : une fuite de données massive qui révèle où sont les risques*, disponible sur : https://www.ldh-france.org/europol-fuite-donnees-massive-revele-les-risques/ (date de la dernière consultation : 02 août 2021).
[162] Entretien avec Pieter-Jan De Grave, Data Protection Officer de la police fédérale belge, annexe I.

collecte et de traitement massifs de données personnelles peuvent avoir sur les personnes concernées, sans pour autant réduire les capacités opérationnelles d'Europol[163].

Enfin, dans un futur proche, des problèmes liés aux mégas-données pourraient survenir avec la mise en place de systèmes d'intelligence artificielle au sein d'Europol. L'intelligence artificielle utilisée à des fins de police prédictive et dotée d'algorithmes capables d'anticiper et de prédire des comportements criminels, peut poser de véritables challenges en matière de protection de données personnelles. En effet, afin que les algorithmes soient performants, il est essentiel de les alimenter d'un volume massif de données d'individus dont la majorité n'a aucun lien avec une quelconque enquête policière. Là, il y a un réel risque que le recueil massif de données personnelles engendre des conséquences négatives pour les citoyens. Selon Pieter-Jan De Grave, l'intelligence artificielle n'est pas encore pleinement utilisée au sein de la police en Europe, mais dans une certaine mesure nous y arrivons[164]. En vertu de la proposition de modification du règlement Europol que nous analyserons dans le dernier chapitre de ce mémoire, Europol jouera très prochainement un rôle clé dans le développement de nouvelles technologies basées sur l'intelligence artificielle dont les services répressifs nationaux pourront profiter. Les technologies d'intelligence artificielle risquent, d'une part, d'augmenter plus que jamais auparavant la partialité et la discrimination à l'égard de certaines catégories d'individus et, d'autre part, de fragiliser notre société démocratique en introduisant des systèmes de surveillance de masse. Par conséquent, ces nouvelles technologies devraient être mises en place uniquement après l'introduction, par le législateur européen, de garanties suffisantes mettant en balance les mesures de surveillance et les conséquences qu'elles pourraient avoir sur notre société[165].

Section 3 : The Zero-Sum Game

Le phénomène du *Big data* a un impact direct sur la coopération policière puisqu'il améliore de façon considérable la collaboration entre les différents services de renseignement étatiques ou non-étatiques et facilite la collecte, le traitement et l'échange d'informations entre eux[166]. En effet, grâce

[163] European Data Protection Supervisor, *opcit.*, pt. 5.
[164] Entretien avec Pieter-Jan De Grave, Data Protection Officer de la police fédérale belge, annexe I.
[165] CCBE, Position du CCBE sur la proposition de règlement modifiant le règlement (UE) 2016/794 en ce qui concerne la coopération d'Europol avec les parties privées, le traitement de données à caractère personnel par Europol à l'appui d'enquêtes pénales et le rôle d'Europol en matière de recherche et d'innovation, 6 mai 2021, p.7.
[166] P. BERTHELET, « Europol face au défi des « méga-données » - L'évolution tendancielle d'une coopération policière européenne « guidée par le renseignement » », *R.D.U.E.*, 2019/2, pp. 157-159.

aux technologies du *Big data*, Europol est en mesure de traiter rapidement la masse de données qu'il collecte, ce qui lui permet d'être plus efficace dans la prévention des formes graves de criminalité. « L'intensification de l'échange d'informations et la technologie sont intimement liées, surtout au regard du phénomène du *Big data*. L'objectif est, grâce aux outils de tri d'un volume massif de données, combiné à des techniques d'analyses toujours plus performantes, d'anticiper les phénomènes criminels »[167]. Par conséquent, au sein d'Europol, les technologies du *Big data* sont en principe mises en place afin d'augmenter la sécurité et la protection des citoyens européens.

Comment Europol peut-il combiner les technologies du *Big dat*a avec la protection des données à caractère personnel, sans pour autant que cette protection ne porte préjudice à la coopération policière ? Au sein de l'Union européenne, le terme de *Zero-Sum* est utilisé pour mettre en lumière ce dilemme complexe, cette lutte constante entre la vie privée des citoyens et le besoin d'augmenter la sécurité en Europe. Il s'agit de la crainte que toutes les garanties qui sont ajoutées à la protection des données personnelles, se soustraient à la sécurité et vice-versa. Le but du *Zero-Sum Game* est d'arriver à mettre en place des garanties à la protection des données personnelles, sans pour autant que cet ajout ait pour conséquence indirecte la réduction de l'efficacité des enquêtes pénales[168].

L'exemple le plus récent du *Zero-Sum Game* est la jurisprudence de la Cour de justice *Data Retention*[169] qui illustre l'évolution des mentalités vis-à-vis de la nécessité de protéger le citoyens européen contre les techniques modernes de surveillance électronique utilisées pour assurer la sécurité publique[170]. Pour des raisons de protection des données à caractère personnel, cette jurisprudence a notamment privé les enquêteurs de certains de leur moyens d'investigation qu'ils estimaient nécessaires pour la sauvegarde de la sécurité européenne et de la lutte contre la criminalité et le terrorisme. En Belgique, elle a eu pour conséquence l'augmentation des perquisitions autorisées par les juges d'instruction. Étant donné que les enquêteurs se sont vus privés de certains de leurs moyens d'investigation, tels que la difficulté d'accéder aux données personnelles d'un suspect directement chez les opérateurs, ils ont détourné le problème en

[167] P. BERTHELET, *opcit.*, p. 187.
[168] Entretien avec Pieter-Jan De Grave, Data Protection Officer de la police fédérale belge, annexe I.
[169] C.J.U.E., arrêt du 6 octobre 2020, *Privacy International*, aff. C-623/17, ECLI:EU:C:2020:790 ; C.J.U.E., arrêt du 6 octobre 2020, *La Quadrature du Net e.a.*, aff. jointes C-511/18, C-512/18 et C-520/18, ECLI:EU:C:2020:791.
[170] M. ROJSZCZAK, « The uncertain future of data retention laws in the EU: Is a legislative reset possible? », *Computer Law & Security Review*, vol. 41, 2021, p.1.

saisissant l'ordinateur du suspect lors d'une perquisition à son domicile[171]. Cette jurisprudence exprime le dilemme du *Zero-Sum* et contribue significativement à la mise en place d'une norme européenne pour la protection des personnes contre les formes modernes de surveillance électronique[172].

Selon Pieter-Jan De Grave, il existe des moyens qui offrent une conciliation possible entre la sécurité et la protection des données personnelles. Par exemple, *The Cloud Act*[173] aux USA est une législation sécuritaire mise en place afin que les autorités américaines puissent accéder aux données des plateformes Internet, comme Facebook et Google. D'un côté, cette législation contribue à l'augmentation de la sécurité du fait que les enquêteurs accèdent plus facilement et plus rapidement aux informations et, de l'autre côté, la protection des données augmente également parce que les recherches seront beaucoup plus ciblées et donc moins massives. Restons tout de même vigilants face à cette législation qui a déjà reçu une montagne de critiques et qui soulève de vives inquiétudes notamment concernant le non-respect de certains droits fondamentaux.

Section 4 : Vers une surveillance et un contrôle de masse ?

La Ligue des droits de l'Homme et d'autres collectifs citoyens ont mis en garde, à de nombreuses reprises, les citoyens et les politiques, des dangers que pouvaient représenter la collecte, le traitement et l'échange massif de données personnelles à l'échelle transnationale. Dans l'opinion publique, ce processus s'apparente plus à une forme de contrôle et de surveillance de masse des individus, plutôt qu'à un dispositif mis en place uniquement pour lutter contre les formes graves de criminalité. Selon l'officier en charge de la protection des données au sein de la police fédérale, cette crainte publique est fondée car il y a des instances européennes qui ont des pratiques pouvant être vues - non pas comme une surveillance de masse - mais comme une surveillance ciblée très invasive ou un traitement de données massif. Certaines technologies de *Big data,* telles que les caméras ANPR, les drones policiers et les antennes de géolocalisation, proposent une surveillance assez invasive permettant de suivre les moindres faits et gestes d'un individu. Cependant, selon ce même officier, nous avons en Europe des garanties et des règles qui encadrent

[171] Entretien avec Pieter-Jan De Grave, Data Protection Officer de la police fédérale belge, annexe I.
[172] M. ROJSZCZAK, *opcit.*, p. 2.
[173] The Clarifying Lawful Overseas Use of Data Act.

la surveillance et qui empêchent les services de polices européens - dont Europol - de tomber dans les travers de la Chine et de la CIA[174].

De manière générale, lors d'un débat autour de la surveillance de masse, l'argument « je n'ai rien à cacher » revient souvent sur le tapis pour exprimer une non-inquiétude vis-à-vis du contrôle opéré par les services de police sur la vie privée des citoyens. Mais pourquoi cet argument est fondamentalement erroné ? Pourquoi avons-nous tous quelque chose à cacher ? Le lanceur d'alerte américain, Edward Snowden, connu pour avoir dénoncé le programme de surveillance de masse mis en place par la NSA[175], a sorti un livre dans lequel il insiste sur l'importance de la vie privée des citoyens. Selon lui, « clamer qu'on n'a pas besoin de vie privée car on n'a rien à cacher, revient à dire que personne ne devrait avoir le droit de cacher quoi que ce soit... Finalement, prétendre que vous n'accordez aucune importance au concept de vie privée parce que vous n'avez rien à cacher, n'est pas très différent que d'affirmer que vous n'avez que faire de la liberté d'expression parce que vous n'avez rien à dire ou que la liberté de culte vous indiffère puisque vous ne croyez pas en Dieu, ou encore que vous vous moquez éperdument de la liberté de réunion parce que vous êtes agoraphobe, paresseux et anti sociable. Si cette liberté ne représente peut-être pas grand-chose pour vous aujourd'hui, cela ne veut pas dire qu'elle ne représentera toujours rien demain »[176]. En effet, aujourd'hui vous pouvez penser, en bon père de famille, que vous ne faites rien de mal, que vous n'avez rien à cacher et que, par conséquent, vous n'accordez pas beaucoup d'importance à la vie privée mais est-ce que cela sera-t-il toujours le cas demain ? Il y a quelques mois, par exemple, se rendre au cinéma ou dans un restaurant sans être vacciné était tout à fait légal et aujourd'hui ce même comportement est devenu punissable par la loi.

De plus, comment être certain que les données personnelles qui ont été collectées par Europol pour une finalité précise, ne seront finalement pas utilisées dans un autre but que celui d'origine ? Par exemple, l'Union européenne a décrété que les empreintes digitales de tous citoyens européens voulant faire un passeport, devaient être obligatoirement enregistrées. Bien qu'à sa mise en place, la finalité première de cette législation était d'éviter les fraudes d'identités, aujourd'hui les empreintes digitales peuvent être utilisées à des fins d'enquête policières, entre autres, aux Pays-

[174] Entretien avec Pieter-Jan De Grave, Data Protection Officer de la police fédérale belge, annexe I.
[175] *National Security Agency* est l'Agence nationale de la sécurité responsable entre autre du renseignement d'origine électromagnétique et de la sécurité des systèmes d'information du gouvernement américain.
[176] E. SNOWDEN, *Permanent Record*, New York City, Metropolitan books, 2019.

Bas. Par conséquent, il nous parait naïf de penser que nous sommes, en tant que citoyens européens, en mesure de prévoir les utilisations futures de nos données à caractère personnel et ce, malgré les législations mises en place pour les protéger[177].

Chapitre 2 : Garanties mises en place par Europol afin d'assurer la protection des données à caractère personnel

D'après nos recherches, il apparait qu'en théorie Europol se dote de suffisamment de garanties et de mesures afin d'assurer une protection adéquate des données à caractère personnel traitées. Selon Pieter-Jan De Grave, il est assez difficile d'analyser si Europol mène une action efficace en matière de protection des données à caractère personnel, étant donné que cette efficacité va en grande partie dépendre de l'enquêteur et de la situation pour laquelle une enquête est en cours. Par exemple, il y a des enquêteurs qui vont introduire une demande auprès de Facebook pour avoir accès au profil d'un certain utilisateur et s'il s'avère que leur analyse mène à d'autres utilisateurs, alors l'enquêteur introduira une nouvelle demande auprès de Facebook pour avoir accès à ces profils. Cette façon de faire respecte les principes de minimisation des données et de nécessité. Par contre, il est fort probable que d'autres enquêteurs se diront qu'il est plus facile de demander - au vu du temps que prend la procédure de demande d'accès auprès de Facebook - directement l'accès d'une centaine de profils susceptibles d'être pertinents pour l'enquête en cours, afin d'être certains de ne plus repasser par Facebook[178].

Section 1 : Plan d'action d'Europol

Europol dispose certainement d'un des régimes les plus solides de protection des données existants au sein de l'Union européenne. Toutefois, ses compétences en matière d'activités de traitement des données doivent être modifiées afin d'être parfaitement conformes avec les normes de l'Union européenne ainsi qu'avec les évolutions technologiques. Le tout, sans impacter le soutien opérationnel d'Europol dont les services répressifs nationaux ont besoin pour lutter contre la grande criminalité et le terrorisme.

[177] M. MARTIJN et R. WIJNBERG, « Nee, je hebt wél iets te verbergen », *de Correspondent*, 2013, disponible sur : https://decorrespondent.nl/209/nee-je-hebt-wel-iets-te-verbergen/6428004-ab2d5fc2 (date de la dernière consultation : 03 août 2021).
[178] Entretien avec Pieter-Jan De Grave, Data Protection Officer de la police fédérale belge, annexe I.

Suite à l'enquête du Contrôleur européen de la protection des données au sujet de l'utilisation de *Big data* par Europol, une solidification de la base juridique de l'agence est prévue. Cette modification, en cours de négociation, vise à renforcer le mandat d'Europol afin qu'il soit plus compatible avec le traitement de grands ensembles de données, tout en respectant les droits fondamentaux. Dans ce cadre-là, Europol a mis en place un plan d'action exposant les initiatives actuelles et futures qu'il a instaurées afin de répondre aux attentes du CEPD en matière de collecte, de traitement et d'échange massif de données. Avec ce plan d'action, Europol est déterminé d'une part, à renforcer la sécurité européenne et d'autre part, à continuer d'offrir un précieux soutien opérationnel aux États-membres et aux autres partenaires, tout en assurant une protection des données conforme aux attentes du CEPD[179].

Les aspects principaux de ce plan d'action concernent les principes fondamentaux de la sécurité des données ainsi que le renforcement des contrôles de la protection des données, permettant de réduire les risques que le traitement massif de données peut avoir pour les personnes concernées. Europol a prévu la mise en place de cinq actions afin de conformer le traitement de grands ensembles de données avec le respect des droits fondamentaux. Toutes ses actions visent à renforcer la protection des données collectées ainsi qu'à restreindre l'accès aux données à caractère personnel aux agents d'Europol. Dans le cadre de l'échange de données avec les États-membres et les autres partenaires de coopération opérationnelle, nous y retrouvons, par exemple, une action permettant de mettre en place un meilleur étiquetage des données entrant dans le réseau SIENA afin de connaître dès le départ la nature des données collectées[180].

Le 16 juin 2021, le CEPD a commenté le plan d'action d'Europol pour que l'Office puisse le modifier et le rendre le plus efficace possible. Dans l'ensemble, le Contrôleur européen est plutôt satisfait des mesures qui ont été proposées par Europol et qui - pour certaines- ont déjà été mises en place. Toutefois, le CEPD reste préoccupé par la possibilité pour Europol de prolonger le stockage de grands ensembles de données, sans procéder à une évaluation de leur conformité avec les restrictions contenues dans le règlement Europol. Pourtant, le Contrôleur européen avait explicitement demandé la mise en place d'une limite de temps maximale pour le stockage de tels ensembles de données, ainsi que des critères précis pour évaluer la nécessité d'une éventuelle

[179] *Ibid.*, p. 8.
[180] Europol, Europol Action Plan addressing the risks raised in the European Data Protection Supervisor (EDPS) Decision on 'Europol's Big Data challenge', doc. 1131384, La Haye, 17 novembre 2020, pp. 2-6.

prolongation de stockage. Malheureusement, sans ces garanties, il y a un risque élevé que les dispositions du règlement Europol ne soient pas totalement respectées[181].

Section 2 : Contrôle opéré par le CEPD

À l'instar de ce que nous avons déjà vu dans ce mémoire, le contrôleur européen de la protection des données est doté, depuis le 1er mai 2017, de deux missions principales. D'une part, il est chargé de vérifier que le traitement des données opéré par Europol soit conforme avec les dispositions du règlement Europol en matière de protection des données. D'autre part, il joue le rôle de conseiller en matière de traitement des données personnelles[182]. En vertu de l'article 43 du règlement Europol, le CEPD peut notamment saisir l'Office en cas de violation des normes de protection de données et émettre des conseils tendant à remédier à cette violation ainsi qu'adresser un avertissement à Europol. Le CEPD est également doté de la capacité d'interdire à Europol de procéder à des activités non conformes aux dispositions régissant le traitement des données à caractère personnel.

Le CEPD travaille en étroite collaboration avec les autorités de contrôle nationales pour assurer une application cohérente du règlement Europol dans toute l'Union européenne[183]. De plus, toute personne a le droit d'introduire une réclamation auprès du CEPD en cas de traitement par Europol de données la concernant et n'étant pas conformes au règlement (UE) 2016/794[184]. Après examen de la réclamation par le CEPD, l'autorité de contrôle nationale avertit la personne concernée du résultat de la réclamation.

Par conséquent, au sein d'Europol, cette structure indépendante, transparente et efficace, est indispensable pour garantir le respect du droit à la protection des données personnelles[185].

Section 3 : Contrôle parlementaire

Au fil de temps, Europol s'est vu conféré davantage de prérogatives. Le Parlement européen devenant préoccupé à l'idée qu'un « embryon d'une police fédérale européenne se développe hors

[181] W. WIEWIOROWSKI, Remarks at the LIBE meeting on the follow-up to the EDPS admonishment Europol, European Data Protection Supervisor, 16 juin 2021, p.2.
[182] Règlement Europol, article 43, §1er.
[183] Règlement Europol, considérant n°51.
[184] Règlement Europol, article 47, §1er.
[185] Règlement Europol, considérant n°50.

de tout contrôle effectif »[186], a rendu pressant le besoin d'un contrôle parlementaire. Le règlement Europol est l'initiative législative qui a contribué sensiblement à améliorer le contrôle parlementaire au sein de l'Office, permettant ainsi de « renforcer la légitimité démocratique et la responsabilité d'Europol envers les citoyens de l'Union »[187].

Le règlement Europol régit le contrôle parlementaire en son chapitre VIII. Le Parlement européen, en collaboration avec les parlements nationaux, contrôle les activités de l'Office. Ensemble, les différents parlements assurent une surveillance politique des incidences que les activités d'Europol peuvent potentiellement avoir sur les libertés et les droits fondamentaux des individus. Ainsi, le contrôle parlementaire se présente comme une garantie supplémentaire au respect du droit à la protection des données.

Chapitre 3 : Proposition de règlement du Parlement européen et du Conseil modifiant le règlement (UE) 2016/794 en ce qui concerne la coopération d'Europol avec es parties privées, le traitement de données à caractère personnel par Europol à l'appui d'enquêtes pénales et le rôle d'Europol en matière de recherche et d'innovation

La proposition de révision du règlement Europol actuellement applicable, fondée sur la base juridique de l'article 88 du T.F.U.E., a pour objectif de réviser le mandat de l'office de police. Cette révision est rendue nécessaire par la complexité et l'évolution des menaces qui mettent en danger la sécurité de l'Union européenne. Le terrorisme représente encore, comme le démontrent les attentats perpétrés à Paris le 25 septembre 2020, à Nice le 29 octobre 2020 ou encore à Vienne le 2 novembre 2020, une menace grave pour les citoyens de l'Union européenne. Depuis peu, une nouvelle menace est apparue sur le plan international, la crise de la COVID-19 qui a eu des répercussions considérables sur la criminalité organisée, en ce sens que « les criminels ont rapidement saisi les opportunités d'exploiter la crise en adaptant leurs modes opératoires ou en développant de nouvelles activités criminelles »[188]. En effet, les criminels ont profité du fait que

[186] P. BERTHELET, « Europol à l'épreuve du secret. Dépassement du modèle intergouvernemental, respect de l'État de droit et accroissement du contrôle démocratique », *OpenEdition*, 2019, pp.5-6.
[187] Règlement Europol, considérant n° 2.
[188] Europol, *Pandemic profiteering how criminals exploit the COVID-19 crisis*, mis en ligne le 27 mars 2020, disponible sur : https://www.europol.europa.eu/publications-documents/pandemic-profiteering-how-criminals-exploit-covid-19-crisis (date de la dernière consultation : 22 juin 2021). Traduit de l'anglais « *Criminals have quickly*

l'attention des services répressifs soit tournée presque exclusivement sur la crise sanitaire pour sévir dans les domaines suivants : la cybercriminalité, la fraude, la contrefaçon de produits sanitaires et pharmaceutiques et d'équipements de protection individuelle ainsi que dans le domaine de crime organisé contre les biens[189]. De plus, les nouvelles technologies telles que les réseaux mobiles 5G, les drones, le cryptage ou encore l'intelligence artificielle, la mondialisation et l'inter-connectivité, sont des moyens qui avantagent les criminels et qui sont exploités par ces derniers pour perpétrer leurs crimes. Par conséquent, il est impératif, selon le Parlement européen et le Conseil, de renforcer les pouvoirs d'Europol afin de lui faciliter la tâche dans sa lutte contre les formes graves de criminalité et de terrorisme ainsi que lui donner les moyens de s'adapter aux menaces nouvelles[190].

La proposition de modification du règlement Europol est intéressante à analyser dans le cadre de ce mémoire étant donné que la quasi-totalité des révisions abordées au sein de cette proposition, impliquent le traitement des données à caractère personnel par Europol. Selon cette initiative législative, les droits fondamentaux tels que le droit à la protection des données à caractère personnel, consacré à l'article 8 de la Charte des droits fondamentaux de l'Union européenne et le droit à la vie privée, consacré à l'article 7 de la Charte, vont bénéficier d'un contrôle strict afin d'assurer leur respect. Concrètement, l'initiative législative dont il est question dans ce chapitre comprend plusieurs modifications du règlement Europol. Elle confère des nouvelles missions à l'Office européen de police et consolide le cadre de protection des données à caractère personnel applicable à Europol.

Premièrement, la proposition de modification du règlement aimerait rendre la coopération entre l'agence et les parties privées plus efficace en autorisant l'échange et l'analyse de données à caractère personnel entre eux[191]. Rappelons que l'échange de données personnelles entre Europol et des parties privées est déjà d'application - conformément à l'article 26 du règlement Europol - mais cet échange n'est autorisé que sous réserve de conditions spécifiques. Les modifications

seized the opportunities to exploit the crisis by adapting their modes of operation or developing new criminal activities ».

[189] *Ibid.*

[190] Proposition de règlement du Parlement européen et du Conseil modifiant le règlement (UE) 2016/794 en ce qui concerne la coopération d'Europol avec les parties privées, le traitement de données à caractère personnel par Europol à l'appui d'enquêtes pénales et le rôle d'Europol en matière de recherche et d'innovation (ci-après « Proposition de règlement modifiant le règlement (UE) 2016/794 »), p.1.

[191] Proposition de règlement modifiant le règlement (UE) 2016/794, p. 14.

apportées par la proposition de règlement ont vocation d'élargir les possibilités légales de ces échanges. Il en découle qu'Europol serait apte à analyser des données à caractère personnel, directement reçues des parties privées, afin d'être en mesure d'identifier les États-membres concernés par ces données et à leur apporter les informations utiles pour établir leur compétence. De surcroît, Europol serait habilité à solliciter les États-membres afin que ces derniers obtiennent toutes données à caractère personnel manquantes et/ou complémentaires auprès de parties privées présentes sur leur territoire. Cependant, l'accès à ces données devrait être strictement limité à ce qui est nécessaire à Europol pour l'accomplissement de ses missions[192].

Deuxièmement, le Parlement européen et le Conseil se sont prononcés sur leur envie de renforcer le rôle d'Europol en matière de recherche et d'innovation, en lien avec ses objectifs. Pour ce faire, l'Office devrait être en mesure d'apporter son soutien aux États-membres afin que ces derniers puissent utiliser efficacement les technologies émergentes qui pourraient les aider à combattre les formes graves de criminalité. L'agence serait également habilitée à traiter des données personnelles, en vue de mettre en œuvre des activités d'innovation, mais uniquement si ce traitement s'avère nécessaire. Toute donnée à caractère personnel nécessitant un traitement dans le cadre d'un projet de recherche et d'innovation d'Europol « relatives à des questions relevant du présent règlement pour l'élaboration, l'entraînement, l'expérimentation et la validation d'algorithmes pour la mise au point d'outils »[193], sera conservée temporairement au sein d'une base de données spécifique dont l'accès sera autorisé uniquement aux membres habilités du personnel d'Europol[194]. De plus, aucun transfert à des personnes non habilitées ni aucune consultation de ces données par d'autres parties ne seront autorisés[195]. Enfin, les données personnelles traitées lors d'un projet de recherche ou d'innovation seront immédiatement supprimées de leur base de données, une fois le projet terminé[196].

Troisièmement, l'initiative législative désire permettre à Europol de traiter des données à caractère personnel figurant dans un dossier d'enquête et recueillies par les États-membres ou par le Parquet européen, afin de les aider à résoudre des enquêtes pénales. Pour que l'Office européen de police puisse intervenir dans une enquête pénale, il est requis qu'un État membre ou le Parquet

[192] Proposition de règlement modifiant le règlement (UE) 2016/794, article 26*bis*, §5.
[193] Proposition de règlement modifiant le règlement (UE) 2016/794, article 18, §2, e).
[194] Proposition de règlement modifiant le règlement (UE) 2016/794, article 33*bis*, §1er, c).
[195] Proposition de règlement modifiant le règlement (UE) 2016/794, article 33*bis*, §1er, d).
[196] Proposition de règlement modifiant le règlement (UE) 2016/794, article 33*bis*, §1er, f).

européen lui demande de l'aide. Europol devrait évidement soutenir une enquête pénale pour être autorisé à analyser l'ensemble de données vastes et complexes se trouvant dans le dossier[197]. De surcroît, il serait possible pour Europol de « conserver le dossier d'enquête et les résultats de son analyse opérationnelle exclusivement aux fins de garantir l'exactitude, la fiabilité et la traçabilité du processus de renseignement criminel et uniquement tant que la procédure judiciaire relative à l'enquête pénale en question est en cours dans un État membre »[198]. L'article 18*bis* de la proposition de règlement, modifiant le règlement (UE) 2016/794, a été introduit à la suite du rapport du CEPD concernant le « défi que représentent les méga- données pour Europol »[199] déjà énoncé dans le mémoire et sera certainement la modification du cadre de protection des données à caractère personnel qui aura le plus d'influence sur le traitement des données[200]. En ce qui concerne l'analyse des méga-données, elle serait facilitée en permettant à Europol d'examiner au préalable la masse importante de données à caractère personnel reçues afin d'évaluer si le traitement de ces données est autorisé. En d'autres termes, l'Office serait en mesure d'analyser les données en question dans le but de vérifier si elles portent sur les catégories de personnes concernées pertinentes, listées à l'article 18, paragraphe 5, du règlement Europol.

Pour finir, le cadre de protection des données à caractère personnel devrait être renforcé par la proposition de modification du règlement Europol. Certaines dispositions[201] du règlement (UE) 2018/1725 relatif à la protection des personnes physiques à l'égard du traitement des données opérationnelles à caractère personnel par les institutions, organes et organismes de l'Union, seraient désormais applicables à Europol. Les catégories particulières de données dites « sensibles », bénéficiant d'une protection supplémentaire, devraient être étoffées par l'ajout de données biométriques en leur sein[202]. Toujours dans la même optique, une nouvelle disposition concernant le traitement de données à caractère personnel à des fins de recherche et d'innovation, devrait être insérée au sein du règlement. Étant donné que le rôle de l'Office dans les domaines de la recherche

[197] Proposition de règlement modifiant le règlement (UE) 2016/794, article 18*bis*, §2, al. 1er.
[198] Proposition de règlement modifiant le règlement (UE) 2016/794, disponible sur : https://www.senat.fr/europe/textes_europeens/e15489.pdf?fbclid=IwAR2EmVG4Ifp8cEUceFGNRMu1lBHGMayCLFcl8T7qY4fSwKrGvwYMtJ6Hrek, p.15.
[199] European Data Protection Supervisor, EDPS Decision on the own initiative inquiry on Europol's big data challenge, C 2019-0370, Bruxelles, 18 septembre 2020.
[200] European Data Protection Supervisor, Avis du CEPD sur la proposition de modification du règlement Europol, Avis 4/2021, 8 mars 2021, p.11.
[201] Notamment l'article 3 relatif aux définitions et le chapitre IX relatif au traitement des données opérationnelles à caractère personnel.
[202] Proposition de règlement modifiant le règlement (UE) 2016/794, article 30, §2.

et de l'innovation sera renforcé et que cette mission aura des conséquences sur le traitement des données à caractère personnel, il est indispensable – eu égard aux droits fondamentaux - de mettre en place des garanties supplémentaires[203]. Enfin, des articles concernant les missions et les fonctions du délégué à la protections des données d'Europol, devraient être insérés dans le règlement afin d'insister sur l'indispensabilité de cette fonction[204].

Les modifications apportées par la proposition de règlement, n'ont pas vocation à changer la nature de l'Office européen de police. Europol n'est en aucun cas un « FBI européen » mais bien une agence de l'Union européenne destinée à faciliter le travail des services répressifs des États-membres, dans le domaine de la criminalité et du terrorisme[205]. En effet, Europol ne devrait pas se substituer aux États-membres qui resteraient les seuls responsables du maintien de l'ordre public et de la sauvegarde de leur sécurité intérieure[206].

Section 1 : Avis du CEPD suite à la proposition de règlement

Suite à la proposition législative modifiant le règlement Europol présenté par la Commission européenne le 9 décembre 2020, le Comité européen de la protection des données a exposé, dans un rapport, sa position face aux mesures proposées et a également émis des recommandations spécifiques en vue de garantir un équilibre entre les droits fondamentaux - dont le droit à la protection des données à caractère personnel - et les intérêts liés à la sécurité[207].

Concernant la coopération entre Europol et les parties privées, le CEPD remarque que les possibilités légales d'échange de données à caractère personnel ont été élargies. Bien que la proposition de règlement introduise des garanties concernant ces échanges de données en son article 26, paragraphe 6, le CEPD estime que ces garanties sont trop étroites. En effet, elles concernent uniquement le transfert de données à caractère personnel à des parties privées, établies

[203] Proposition de règlement modifiant le règlement (UE) 2016/794, article 33*bis*.
[204] Proposition de règlement modifiant le règlement (UE) 2016/794, articles 41*bis* et 41*ter*.
[205] Sénat, *Proposition de règlement du Parlement européen et du Conseil modifiant le règlement (UE) 2016/794 en ce qui concerne la coopération d'Europol avec les parties privées, le traitement de données à caractère personnel par Europol à l'appui d'enquêtes pénales et le rôle d'Europol en matière de recherche et d'innovation*, disponible sur : https://www.senat.fr/ue/pac/EUR000006727.html?fbclid=IwAR3xJog8FcgTRty55PSFpJA7TxnIey4wx_gK-khd5_yibr96SMdi5Q1m-0U (date de la dernière consultation : 24 juin 2021).
[206] T.F.U.E., article 72 ; Traité sur l'Union européenne (TUE), article 4, §2.
[207] Résumé de l'avis du contrôleur européen de la protection des données sur la proposition de modification du règlement Europol, *J.O.U.E.*, C 143/6, 23 avril 2021.

en dehors de l'Union, alors que le CEPD souhaite que ces garanties soient élargies à l'ensemble des parties privées, qu'elles soient établies dans l'Union européenne ou non[208].

La proposition législative renforce également le rôle d'Europol en matière d'activités de recherche et d'innovation. À cet égard, le CEPD remarque que la portée du traitement des données à caractère personnel, effectué au moyen des projets de recherche et d'innovation[209], est trop large et préconise que la portée de ces activités soit mieux définie. De plus, le Comité européen désire que la liste des garanties contenue à l'article 33*bis* de la proposition, soit vue comme étant une liste non-exhaustive et considérée comme le minimum applicable en matière de protection des données[210].

Par ailleurs, concernant le traitement d'informations à l'appui d'enquêtes pénales, le CEPD s'inquiète de la portée de l'article 18*bis* de la proposition légale. Nous rappelons que cet article propose des dérogations permettant de traiter des données à caractère personnel non contenues dans la liste de l'annexe II du règlement Europol et des dérogations aux délais actuels de conservation des données. Voulant éviter que l'article 18*bis* ne devienne la règle, le CEPD préconise d'introduire des garanties légales, telles que l'importance, le type ou encore la complexité de l'enquête pénale, à cet article. Notons malgré tout que toutes mesures qui dérogent au traitement des données personnelles, doivent se conformer au règlement (UE) 2018/1725 et plus précisément à son chapitre IX[211].

Pour finir, le Comité européen est entièrement satisfait de la proposition de renforcement du cadre de protection des données à caractère personnel, en ce sens qu'elle s'inscrit dans une harmonisation dudit cadre pour les agences, les instituions et les organes de l'Union européenne. Cependant, l'harmonisation des pouvoirs de contrôle du CEPD, conférés à l'article 58 du règlement (UE) 2018/1725 à l'égard des activités d'Europol, n'est toujours pas d'actualité avec la proposition

[208] European Data Protection Supervisor, Avis du CEPD sur la proposition de modification du règlement Europol, Avis 4/2021, 8 mars 2021, p.9.
[209] Proposition de règlement modifiant le règlement (UE) 2016/794, article 18, §2, e).
[210] European Data Protection Supervisor, Avis du CEPD sur la proposition de modification du règlement Europol, Avis 4/2021, 8 mars 2021, p.12.
[211] European Data Protection Supervisor, Avis du CEPD sur la proposition de modification du règlement Europol, Avis 4/2021, 8 mars 2021, p.12.

de règlement. Subséquemment, le CEPD requiert que l'article 58 du règlement (UE) 2018/1725 soit applicable, dans son entièreté, à Europol[212].

Section 2 : Avis du Conseil des barreaux européens suite à la proposition de règlement

Le Conseil des barreaux européens (ci-après le « CCBE) a également exposé sa position suite à la proposition de règlement. Il craint que l'invocation, par les services répressifs nationaux, d'une prétendue menace à la sécurité nationale - telle qu'une attaque terroriste - ne soit en réalité, utilisée uniquement pour avoir accès à des données à caractère personnel dont l'accès est normalement limité, voir interdit. « Le terrorisme était bien entendu invoqué pour justifier l'adoption par l'État de la plupart des programmes de surveillance, à une époque où régnaient la peur et l'opportunisme »[213]. Pour pallier à cette problématique et assurer l' état de droit, le CCBE suggère d'adopter des définitions communes et internationalement acceptées des notions de « terrorisme » et de « sécurité nationale » afin que les tribunaux puissent s'assurer que toutes les mesures de surveillance adoptées soient proportionnées et nécessaires face à la menace[214].

Le CCBE s'inquiète également des conséquences que les mesures de l'Union européenne sur l'accès d'Europol aux données à caractère personnel, pourraient avoir sur le secret professionnel ou le *legal professional privilege*. Le Conseil des barreaux européens estime que les fournisseurs d'accès à Internet, n'ont pas les moyens de reconnaître à l'avance si les données demandées par Europol relèvent du secret professionnel, ce qui pourrait mener à des violations dudit secret et, par conséquent, porter indirectement préjudice au droit à un procès équitable garanti par l'article 6 de la Convention européenne des droits de l'homme. Selon le CCBE, la mise en place d'une technologie avancée, capable d'identifier les données relevant du secret professionnel, devrait être une priorité tant pour les parties privées que les services répressifs et Europol. De ce fait, toutes

[212] *Ibid.*, pp. 14-15.
[213] E. SNOWDEN, *Permanent Record*, New York City, Metropolitan books, 2019.
[214] CCBE, Position du CCBE sur la proposition de règlement modifiant le règlement (UE) 2016/794 en ce qui concerne la coopération d'Europol avec les parties privées, le traitement de données à caractère personnel par Europol à l'appui d'enquêtes pénales et le rôle d'Europol en matière de recherche et d'innovation, 6 mai 2021, p.1.

données protégées par le secret professionnel seraient immédiatement écartées de la collecte, de la conservation, du traitement et de l'échange des données à caractère personnel[215].

De plus, le CCBE considère que l'accès aux données personnelles par Europol, en tant qu'agence souhaitant mener une surveillance, doit impérativement être transparent ainsi que soumis à des contrôles législatifs et démocratiques stricts et efficaces. Cet accès ne devrait être autorisée que sous certaines conditions spécifiques clairement définies. Rappelons qu'en vertu de la jurisprudence de la CJUE et du principe de proportionnalité, la lutte contre la criminalité grave et la prévention des menaces graves contre la sécurité publique, sont les seules mesures de sécurité qui justifient des atteintes graves aux droits fondamentaux consacrés aux articles 7 et 8 de la Charte[216]. Le CCBE estime que le contrôle législatif actuellement en vigueur ainsi que celui introduit par la proposition de modification du règlement Europol, ne peuvent pas garantir un contrôle démocratique efficace des activités de l'Office. Le nouveau règlement devrait renforcer les pouvoirs du groupe de contrôle parlementaire conjoint afin qu'il puisse conférer des sanctions à Europol en cas de violation d'un droit fondamental dont le droit à la protection des données personnelles[217].

En conclusion, le CCBE invite Europol à répondre urgemment aux préoccupations que soulève cette proposition législative, en apportant des solutions aux traitements illégaux des données à caractère personnel. De plus, il considère que l'évaluation par la Commission européenne du règlement Europol, devant avoir lieu en 2022 et portant sur l'efficacité de l'Office et de ses méthodes de travail, est l'occasion parfaite pour analyser en profondeur la compatibilité des activités d'Europol avec les droits fondamentaux. En prenant en compte les avis CEPD et du CCBE, l'adoption de la proposition de modification du règlement Europol serait prématurée et hâtive[218].

[215] CCBE, Position du CCBE sur la proposition de règlement modifiant le règlement (UE) 2016/794 en ce qui concerne la coopération d'Europol avec les parties privées, le traitement de données à caractère personnel par Europol à l'appui d'enquêtes pénales et le rôle d'Europol en matière de recherche et d'innovation, 6 mai 2021, pp. 2-3.
[216] CJUE, arrêt du 6 octobre 2020, *La Quadrature du Net e.a.*, affaires jointes C-511/18, C-512/18 et C-520/18, ECLI:EU:C:2020:791, §140.
[217] CCBE, *opcit.*, p.4.
[218] *Ibid.*, p.9.

CONCLUSION

Depuis sa création, Europol a une capacité particulière à s'adapter aux évolutions sociétales et technologiques. En constant renouvellement, l'agence de l'Union européenne ne se repose jamais sur ses acquis afin de proposer la meilleure version d'elle-même. Lors de son entrée en vigueur, le règlement Europol offrait un régime solide de protection des données, en adéquation avec les besoins du terrain et de son époque. Aujourd'hui, face aux avancées technologiques, à la complexité des menaces criminelles et aux autres défis rencontrés par l'Office, cette protection n'est plus suffisante. C'est la raison pour laquelle une proposition de révision du règlement Europol est en cours de négociations. Bien que cette proposition législative soulève quelques préoccupations, elle est nécessaire - voire primordiale - pour la mise en place d'une protection plus solide et transparente des données personnelles qui tiennent compte des nouvelles technologies utilisées par les services répressifs nationaux et par Europol.

Toujours dans le but de promouvoir une « Europe de la sécurité », Europol développe continuellement des technologies innovantes lui permettant de s'adapter aux menaces criminelles. L'utilisation du *Big data* est rapidement devenue indispensable dans le domaine de la sécurité. La mise en place de systèmes permettant la collecte et le traitement massif d'informations était essentielle pour lutter efficacement contre les formes graves de criminalité. Les technologies du *Big data*, dorénavant intégrées au sein d'Europol, sont souhaitées par les États-membres et les institutions européennes. Elles sont en effet favorables à l'intensification des échanges d'informations et à l'augmentation de l'efficacité des analyses criminelles qui peuvent désormais être réalisées en quelques heures seulement. De plus, le traitement d'une large quantité de données permet d'arriver à des analyses plus précises et à des inspections plus ciblées et, par conséquent, à des rendements plus élevés. L'utilisation du *Big data* permet donc à Europol d'accroitre ses capacités en développant des nouvelles techniques afin d'accomplir des tâches impossibles auparavant, telles que la prédiction de crimes[219]. Ralentir l'essor du phénomène d'amplification et d'accélération du processus de collecte et d'échange de données personnelles, n'est pas désirable, ni désiré pour l'efficacité de la coopération policière. Au contraire, Europol va vers un

[219] WRR, « Big Data in een vrije en veilige samenleving », *Amsterdam University Press*, 2016, pp. 77-78.

accompagnement du phénomène du *Big data*, en comblant toutes les lacunes freinant son essor et en investissant dans des systèmes intelligents de collecte et d'échange d'informations[220].

Néanmoins, l'utilisation du *Big data* ne présente pas que des avantages. Nombreux sont les risques rencontrés lors de l'utilisation des nouvelles technologies et la protection des données à caractère personnel est en tête de liste. Le traitement rapide d'un trop grand volume de données a des répercussions sur la vie privée des individus et sur la vie privée en tant que valeur sociale. Le risque de violation de la vie privée - en ce compris celui de la protection des données à caractère personnel - est majeur dans l'application des processus du *Big data*. En général, le contenu des données collectées par Europol demeure inconnu jusqu'au moment où l'analyse est menée. Par conséquent, le risque que ces données appartiennent à des personnes ne se trouvant pas dans la liste de l'annexe II B du règlement Europol est élevé. Cette annexe concerne les catégories de données personnelles pouvant être collectées et traitées et les catégories de personnes concernées dont les données peuvent être collectées et traitées[221]. En d'autres termes, Europol stocke, au sein de ses serveurs, des données appartenant à des personnes n'ayant strictement aucun lien avec une quelconque activité criminelle[222]. Ce stockage à grande échelle peut potentiellement causer du tort aux personnes concernée, dont les données se retrouvent dans des fichiers initialement réservés aux activités criminelles. Dès lors, leur vie privée, professionnelle et familiale ainsi que leur libre circulation, peuvent être impactées.

De plus, le traitement massif de données personnelles est en contradiction avec le principe de limitation de la finalité, en vertu duquel les données ne peuvent être utilisées qu'à des fins spécifiques, explicites et justifiées[223]. Il est également en contradiction avec le principe général de la minimisation des données qui veut que la collecte de données à caractère personnel soit adéquate, pertinente et strictement limitée à ce qui est nécessaire, au regard des finalités de traitement[224]. L'étude des risques rencontrés lors de l'utilisation du *Big data* a poussé le CEPD à conclure à l'impossibilité pour Europol de garantir la protection de toutes les données contenues en son sein.

---

[220] P. BERTHELET, « Europol face au défi des « méga-données » - L'évolution tendancielle d'une coopération policière européenne « guidée par le renseignement » », *R.D.U.E.*, 2019/2, p. 187.
[221] European Data Protection Supervisor, EDPS Decision on the own initiative inquiry on Europol's big data challenge, C 2019-0370, Bruxelles, 18 septembre 2020, pt. 4.10 et 4.11.
[222] *Ibid.*, pt. 4.7 et 4.8.
[223] WRR, « Big Data in een vrije en veilige samenleving », *Amsterdam University Press*, 2016, p.90.
[224] RGPD, article 5, §1er, c).

Nous avons également constaté que le recours à des technologies utilisant du *Big data*, telles que les caméras ANPR, les drones policiers et les antennes de géolocalisation, permettent à Europol et aux services répressifs d'avoir plus de connaissances sur les citoyens européens. Dans le domaine de la sécurité, cette connaissance peut avoir un effet intimidant si elle devient trop importante. Il en découle que dans l'opinion publique, la crainte que l'utilisation du *Big data* s'apparente plus à une forme de contrôle et de surveillance de masse, plutôt qu'à un dispositif mis en place uniquement pour lutter contre les formes graves de criminalité, est réelle. Cependant, nous avons ressenti lors de nos interviews que le débat autour d'une éventuelle surveillance de masse opérée par Europol est très sensible. D'une part, le *Data Protection Officer* de la police fédérale belge comprend la crainte des citoyens et admet que certaines technologies utilisées par les services répressifs, proposent une surveillance invasive. Néanmoins, il considère que nous avons en Europe des garanties qui encadrent la surveillance et qui empêchent Europol de tomber dans les travers de la Chine et de certaines agences telle que la CIA[225]. D'autre part, le *Data Protection Officer* d'Europol considère qu'il n'est pas approprié de mentionner la surveillance de masse lors d'une analyse sur l'Office européen de police. Il nous parait donc indispensable de mettre en lumière les risques liés au traitement massif de données, quels qu'ils soient, d'une part, pour que l'utilisation du *Big data* soit socialement acceptable et, d'autre part, afin d'instituer les garanties nécessaires à son utilisation.

Dans notre société informatisée, la protection des données à caractère personnel est sous pression, tant de la part des entreprises, des services répressifs que des agences de l'Union européenne et le *Big Data* intensifie cette pression. Le traitement à grande échelle de données personnelles provoque au quotidien des violations mineures de la protection des données, si petites qu'elles ne sont pas suffisantes pour pouvoir entraîner des poursuites judiciaires à elles seules. Cependant, lorsque toutes ces petites violations sont additionnées, le préjudice causé au droit fondamental de la protection des données est considérable. L'accent devrait donc être mis sur le préjudice collectif causé au droit fondamental plutôt que sur le préjudice individuel causé aux personnes concernées[226].

[225] Entretien avec Pieter-Jan De Grave, Data Protection Officer de la police fédérale belge, annexe I.
[226] WRR, « Big Data in een vrije en veilige samenleving », *Amsterdam University Press*, 2016, p.91.

Tout au long de ce mémoire, nous nous sommes heurtés à un paradoxe ; le respect du droit fondamental qui est celui de la protection des données personnelles et le besoin d'adopter - pour des raisons de sécurité publique - des techniques permettant la collecte et le traitement massif de données. Nous avons remarqué que le renforcement des mesures de protection des données personnelles au sein de l'Union européenne, pouvait entrainer des conséquences négatives pour la coopération policière et nuire à l'efficacité des enquêtes criminelles. Le but ultime d'Europol devrait être de renforcer la protection des données personnelles, sans pour autant impacter négativement son efficacité dans le cadre de la prévention de la criminalité[227].

En conclusion, la question est de voir comment Europol peut-il combiner le recueil et le traitement massif d'informations avec la protection des données à caractère personnel ? Nous avons vu qu'Europol dispose d'un des régimes les plus solides en matière de protection des données au sein de l'Union européenne. Nous avons également vu qu'Europol - pleinement conscient des défis posés par la collecte et le traitement massif de données - prépare une proposition de règlement modifiant le règlement Europol. Cette initiative législative, ayant vocation de consolider le cadre de la protection des données au sein d'Europol, ainsi qu'à renforcer les pouvoirs de l'agence, a été proposée afin qu'Europol puisse s'adapter aux évolutions technologiques et aux nouvelles menaces. Nous pensons que cette proposition législative est une solution pertinente à la problématique rencontrée par Europol mais qu'elle n'est pas suffisante, à elle seule, à garantir une protection des données adéquate.

À l'heure actuelle, nous ne sommes pas convaincus par l'efficacité de l'Office européen de police à garantir une protection des données personnelles adéquate. Nous rejoignons pleinement l'avis du CEPD exposé dans son enquête du 30 avril 2019, selon lequel Europol n'a pas les moyens de s'assurer que l'ensemble des données collectées, soit conforme aux normes de protection des données[228]. Pleinement conscients de la difficulté pour Europol de combiner le traitement massif de données avec leur protection - le tout, sans impacter l'efficacité de son soutien opérationnel dans la lutte contre la grande criminalité et le terrorisme - nous ne blâmons pas l'Office. Nous nous

[227] D. DREWER et V. MILADINOVA, « The BIG DATA Challenge: Impact and opportunity of large quantities of information under the Europol Regulation », *Computer Law & Security Review*, vol. 33, 2017, p. 308.
[228] European Data Protection Supervisor, EDPS Decision on the own initiative inquiry on Europol's big data challenge, C 2019-0370, Bruxelles, 18 septembre 2020, pt. 4.7.

demandons, par contre, si le principe même du *Big data* n'est pas diamétralement opposé aux normes sociales et juridiques actuelles sur la protection des données.

Dans un futur proche, nous craignons que les évolutions technologiques dans le secteur de la sécurité, telles que l'intelligence artificielle, impactent les droits fondamentaux des citoyens. L'intelligence artificielle traite des volumes impressionnants de données afin de fonctionner convenablement. Les données de personnes non impliquées dans une activité criminelle risquent d'être utilisées à grande échelle, entrainant des conséquences négatives sur leur vie privée. De manière générale, nous espérons que suffisamment de mesure de contrôle indépendante seront mises en place, tant d'un point de vue légal que politique, afin de garantir le respect continuel des droits fondamentaux.

Annexe I : Entretien avec Pieter-Jan De Grave, Data Protection Officer de la police fédérale belge[229]

Quel est votre rôle au sein de la police fédérale belge et en quoi consiste-t-il ?

Pieter-Jan De Grave : J'occupe plusieurs rôles au sein de la police fédérale belge. Premièrement, j'occupe le poste de juriste au sein du département de coopération bi et multilatérale qui est le département en charge de la coopération directe avec un certain pays. Concrètement, je négocie des traités avec certains pays - j'ai d'ailleurs pris part à la négociation du nouveau traité Benelux - et je travaille en collaboration directe avec le FBI, les collègues étrangers et d'autres agences.

Deuxièmement, je suis le Data Protection Officer pour l'échange international d'informations entre États mais également entre agences internationales et européennes telles qu'Europol et Interpol. Dans ce cadre-là, je regarde tous les aspects de protection des données en lien avec ces échanges d'informations.

Troisièmement, en tant que juriste, je contrôle le cadre pour l'échange d'informations directes. Via des messages des pays étrangers comme la Moldavie, demandent aux services de police belges si une personne X apparait déjà dans leurs systèmes et il s'en suit des discussions par messages.

Aujourd'hui, nous faisons face à un nouveau phénomène, celui des mégas-données (Big Data). Selon vous, quelles sont les raisons qui expliquent cette amplification et cette accélération du processus de collecte et d'échange de données à caractère personnel ?

Pieter-Jan De Grave : Ce phénomène est largement dû à l'évolution technologique que connait notre société et à la révolution digitale (*the digital age)*. Il faut être conscient qu'au sein de la police, on a toujours eu besoin d'informations pour résoudre des enquêtes. En effet, l'information est considérée comme la base et le moteur de la police. À l'heure actuelle, avec la révolution digitale, on remarque une amplification des données. Cela est dû, d'une part, à la digitalisation de la société et aux données mises en ligne (profil Facebook, adresse e-mail, etc.) qui multiplient massivement les données à disposition des services répressifs et, d'autre part, aux nouveaux

[229] Monsieur De Grave parle en son nom propre et non en celui de la police fédérale belge.

moyens dont la police s'est dotée. Ces nouveaux moyens sont, entre autres, les caméras ANPR (*Automatic Number Plate Recognition*) ou LAPI (Lecteur Automatique de Plaques d'Immatriculation) qui filment en temps réel et prennent une photo de chaque plaque d'immatriculation. Dès qu'il y a une correspondance avec une plaque renseignée dans une banque de données de référence, la police en est immédiatement avertie. Ainsi, la police est en mesure de contrôler chaque voiture qui entre ou qui sort d'une zone déterminée. Par exemple, le Royaume-Unis est doté d'un réseau de caméras placées sur toutes les routes délimitant le pays, leur permettant de la sorte de contrôler chaque voiture qui entre et qui sort de ce pays. Les données sont conservées pendant des dizaines d'années. Les policiers anglais peuvent donc savoir que le 7 décembre 2014 à 16h43 vous avez franchi leur territoire en voiture. De plus, lors d'un cambriolage par exemple, nous pouvons analyser les données des caméras se situant à proximité du lieu du cambriolage afin d'identifier exactement chaque voiture qui est passée à proximité du lieu en question. Cette nouvelle technologie est un moyen permettant de récolter un nombre incalculable d'informations. Le même principe est utilisé pour les données de géolocalisation des téléphones portables. La police place des antennes au-dessus des églises ou au-dessus d'autres bâtiments centraux afin d'analyser les données de toutes personnes étant passées aux alentours de ces antennes. En conclusion, la digitalisation de la société et les nouveaux moyens dont la police s'est dotée, sont pour moi les deux raisons pour lesquelles il y a ce phénomène de *Big Data*.

Quels sont les principaux problèmes que soulève un tel phénomène au regard de la protection des données personnelles ?

Pieter-Jan De Grave : Ce phénomène fait apparaitre deux grands problèmes. Premièrement, pour reprendre le cas d'Europol, l'agence va être amenée à traiter des données de personnes qui ne se trouvent pas à l'annexe II du règlement, c'est-à-dire qui ne se trouvent pas sur la liste de personnes dont Europol est habilité à traiter les données. C'est un problème qui n'en est pas réellement un, étant donné qu'il est « facile » d'y remédier légalement. La proposition de modification du règlement Europol essaye justement de pallier à ce problème en modifiant la liste de l'annexe II. Par contre, le deuxième problème est plus difficile à régler d'un point de vue légal. Il s'agit du principe général de *data minimisation* que l'on retrouve dans de nombreux traités et dans les instruments de protection des données à caractère personnel. Ce principe nous dit que vous

ne pouvez collecter les informations des personnes que si cela s'avère nécessaire au regard de votre enquête.

Nous retrouvons ces deux problèmes dans les technologies dont se sont dotés les services répressifs. Les caméras ANPR collectent un nombre incalculable de données concernant les voitures qui sont passées, par exemple, devant une caméra située à Bruxelles lors du dernier mois. Le problème est qu'il n'y a en général qu'une ou deux plaques d'immatriculation qui vont vous intéresser, alors que la majorité des données collectées vont être liées à des personnes qui n'ont strictement rien à faire avec votre enquête. Les technologies de géolocalisation rencontrent le même problème. Vous vous retrouvez avec des données massives de personnes à analyser, alors que la grande majorité de ces données ne sont pas pertinentes pour votre enquête.

Selon moi, la collecte et le traitement massif des données, ne représentent pas, en soi, un problème, à partir du moment où les règles et les principes de proportionnalité et de nécessité de l'information sont respectés. Le problème survient lorsque les services de police traitent les données de dizaines de milliers de personnes qui n'ont rien à faire avec leurs enquêtes, et les stockent sur leurs serveurs policiers pendant des années. En effet, le fait qu'une personne se retrouve dans une base de données policière, est une information sensible qui peut avoir beaucoup de conséquences pour la personne concernée.

Europol et la police fédérale, vous paraissent-ils mener une action efficace en matière de protection des données à caractère personnel ?

Pieter-Jan De Grave : C'est une question pour laquelle il est assez difficile d'apporter une réponse, étant donné que cela va dépendre de l'enquêteur, de la situation même et de l'agence ou du service répressif pour lequel on travaille. Par exemple, il y a des enquêteurs qui vont introduire une demande auprès de Facebook pour avoir accès au profil d'un certain utilisateur et, si l'analyse de ce profil mène à d'autres utilisateurs, alors l'enquêteur introduira une nouvelle demande auprès de Facebook pour avoir accès à ces profils. Cette façon de faire respecte les principes de *data minimisation* et de nécessité. Par contre, on aura sans doute aussi des enquêteurs qui se diront qu'étant donné que la procédure de demande d'accès auprès de Facebook prend du temps, il vaut mieux demander directement l'accès d'une centaine de personnes qui les intéressent pour être

certains de ne plus repasser par Facebook. Donc ça dépend vraiment de l'enquêteur même et de sa hiérarchie.

Cependant, je pense qu'en général, il y a suffisamment de garanties et de mesures mises en place pour assurer une bonne protection des données à caractère personnel. Il faut dire aussi que les *Data Protection Officer* apportent une garantie supplémentaire, étant donné qu'ils vérifient que les enquêteurs respectent bien les règles.

Selon vous, quel dispositif pourrait être mis en place afin d'assurer une meilleure protection des données personnelles ?

Pieter-Jan De Grave : Honnêtement, je ne sais pas ce qu'on pourrait faire de plus, sauf vraiment commencer à regarder en détail toutes les enquêtes et mettre en place pour chaque enquête un système de vérifications faites par un DPO. Personne ne veut en arriver là et de toute façon ce n'est pas réaliste de mettre en place un système pareil. Le respect de la protection des données personnelles repose surtout sur une question de culture et de sensibilisation de la situation.

À l'heure actuelle, la police est en train de mettre en place un nouveau système, c'est le projet « iPolice » qui devait normalement voir le jour en 2020. L'idée est de refaire tous les systèmes informatiques de la police fédérale ainsi que locale pour qu'ils soient plus conformes à la réalité technique. À mon avis, ce système va contribuer à l'augmentation des garanties de protection des données. En effet, grâce à un système de logs, on sera en mesure de savoir exactement quel agent a consulté, modifié ou supprimé des données dans un système, ainsi que l'heure à laquelle ces manipulations ont été faites. Nous serons obligés d'installer ce système de logs dans tous les systèmes policiers d'ici 2023.

Sachant qu'au plus Europol collecte et traite des données, au plus il est efficace dans la prévention des formes graves de criminalité, pensez-vous que le renforcement de la protection des données à caractère personnel, au sein des services répressifs nationaux et des agences de l'Union européenne (tel qu'Europol), puisse avoir un impact négatif sur la coopération policière ?

Pieter-Jan De Grave : Effectivement et c'est une crainte générale au sein de la police et d'Europol. C'est également la raison pour laquelle nous avons des difficultés à convaincre d'autres pays, tel que la Turquie, de suivre les règles de protection des données que nous suivons en Europe.

Au sein de l'Union européenne, on utilise le terme de *Zero-Sum* qui met en lumière ce dilemme. Il s'agit de la crainte que tout ce que l'on rajoute à la protection des données, se soustrait à la sécurité et vice versa. Le but du *Zero-Sum* est d'arriver à rajouter des garanties d'un côté, sans en perdre de l'autre et donc de rajouter des garanties à la protection des données, sans pour autant perdre l'efficacité des enquêtes pénales.

Comment va-t-on résoudre ce dilemme ? C'est la question à dix millions partout dans l'Union européenne. C'est un dilemme et il est très difficile à résoudre. Récemment, l'exemple le plus clair est la jurisprudence *Data Retention* qui dit que, pour des raisons de protection des données, on va vous prendre certains de vos moyens d'investigations. Parmi les collègues, cette jurisprudence tombe comme un coup de massue et leur donne l'impression que la protection des données est considéré comme étant plus importante que la sécurité.

Il existe des moyens d'augmenter la protection des données personnelles, tout en augmentant l'efficacité des enquêtes policières. *The Cloud Act* aux USA est une législation sécuritaire mise en place afin que les autorités américaines, ainsi que les organisations internationales et les États avec lesquels les autorités américaines ont conclu des traités, puissent accéder aux données des plateformes Internet, comme Facebook et Google. Je reviens vers mon exemple précédent, un enquêteur sachant pertinemment que demander et recevoir des informations de la part de Facebook est une démarche qui prend du temps, sera tenté de demander l'accès à plusieurs profils à la fois, plutôt que de demander uniquement ce qui est nécessaire pour son enquête. Cependant, si l'enquêteur a accès plus rapidement aux informations dont il a besoin, comme ce que propose la législation *The Cloud Act*, il consultera uniquement les profils nécessaires. En conséquence, d'un côté, cette législation augmente la sécurité parce que les enquêteurs peuvent beaucoup plus facilement accéder aux informations et, de l'autre côté, la protection des données augmente également parce que les recherches seront beaucoup plus ciblées. Voilà un exemple qui offre une conciliation possible de la sécurité et de la protection des données personnelles.

Pouvez-vous concevoir que certaines personnes (dont la Ligue des droits de l'Homme et des collectifs citoyens) craignent que ce processus de collecte et d'échange de données personnelles à l'échelle transnationale, puisse s'apparenter plus à une forme de contrôle et de surveillance de masse des individus plutôt qu'à un dispositif mis en place uniquement pour lutter contre les formes graves de criminalité ? Cette crainte est-elle fondée ou sort elle de l'imaginaire des individus ?

Pieter-Jan De Grave : Cette crainte est fondée. Évidemment, il faut faire la distinction entre la surveillance de masse faite par plusieurs institutions et ce qu'Europol et les services de police européens font. Dans nos systèmes européens, on ne fait pas de surveillance de masse, par contre, la crainte est bien fondée parce qu'il y a des instances qui ont des pratiques pouvant être vues, non pas comme une surveillance de masse, mais comme une surveillance ciblée très invasive ou un traitement de données massif. Par exemple, grâce aux caméras ANPR, les enquêteurs peuvent suivre les moindres mouvements d'une voiture partout en Europe. Dans certains dossiers médiatiques d'il y a quelques années, nous avons réussi à suivre le trajet exact de certaines voitures. Pour la surveillance et le contrôle d'une personne, nous avons également les drones dotés de caméras, grâce auxquels les enquêteurs peuvent suivre une personne beaucoup plus facilement qu'avant. Ces technologies proposent une surveillance assez invasive qui n'est pas une surveillance de masse, comme nous pensons que la Chine et la CIA font, mais c'est une surveillance quand même. En Belgique, nous avons des garanties et des règles qui encadrent la surveillance, ce sont les méthodes d'enquêtes particulières qui nous empêchent justement de tomber dans les travers de la Chine et de la CIA.

D'un autre côté, nous pouvons également traiter les données de toute une masse de personnes, au moyen des antennes de géolocalisation dont j'ai parlé précédemment. Ces raisons me poussent à penser que les craintes sont fondées et qu'il y a des risques, il y a des situations où l'on cherche la limite jusqu'où on peut aller. Par contre, il faut toujours trouver la balance et se demander si l'alternative mise en place pour palier à ces problèmes de surveillance, n'est pas pire que l'original. Prenons, par exemple, la jurisprudence *Data Retention*. Cette jurisprudence a diminué les possibilités et les moyens d'enquête des enquêteurs pour privilégier la protection des données à caractère personnel. Quelles ont été les réactions et les conséquences de cette jurisprudence ? Une des conséquences a été que les juges d'instruction ont beaucoup plus facilement demandé une perquisition. Évidemment, si les enquêteurs ne peuvent pas avoir accès aux données d'un suspect directement chez les opérateurs, ils vont devoir faire une perquisition chez le suspect en question et saisir son ordinateur. La réaction provoquée par cette jurisprudence n'est pas souhaitable. Encore une fois, nous recherchons une balance, *Zero-Sum*, entre la sécurité et les garanties de protection des données.

En conclusion, cette crainte est fondée parce qu'il y a de réels risques à la collecte et à l'échange massif de données mais, à nouveau, je veux mettre le point sur la surveillance en masse faite en Chine, cela ne se fait pas chez nous.

Est-ce que la collecte et le traitement massif des données personnelles génèrent des erreurs ou des dysfonctionnements dont les individus sont amenés à pâtir ? Avez-vous un exemple concret auquel vous avez été confronté ?

Pieter-Jan De Grave : Dans mon expérience, non. Il y a des erreurs, je ne peux pas trop aller en détail à cause du secret professionnel mais il y a des situations dans lesquelles nous avons transmis certaines informations à l'étranger sans trop mesurer l'importance de cet échange. Des données qui ont été utilisées pas comme il l'aurait fallu, ce qui a eu des conséquences pas souhaitables ni souhaitées. Je ne parle pas de gros problèmes, il n'y a pas des personnes qui sont décédées à cause de ces erreurs. Je pense à une situation où quelqu'un n'a pas reçu une licence de résidence lui permettant d'habiter et de travailler dans un certain pays, à cause du fait que nous n'avons pas été suffisamment prudents avec l'information que nous avons donnée à ce pays. Nous rencontrons ce genre de situations de temps en temps. Cependant, je n'ai pas encore rencontré de problèmes spécifiquement à cause du *Big data* et des traitements massifs de données.

L'enquêteur va traiter beaucoup de données parce que techniquement il reçoit un fichier énorme dont il doit analyser les données et garder les informations pertinentes. En général, l'enquêteur est seulement intéressé par les données pertinentes avec son enquête et, à partir du moment où il a isolé les données de sa cible, il se « débarrasse » du reste. Un problème se rencontre dans plusieurs pays (ce n'est pas vraiment le cas en Belgique), pour des raisons de vérifications de preuves, la législation Antigone exige des enquêteurs qu'ils gardent toutes les informations qu'ils ont collectées au cours de leur enquête. Évidemment, cette législation pose problème étant donné qu'elle exige la conservation de données de personnes non pertinentes avec les enquêtes de polices.

Les erreurs vont dépendre de la manière dont les informations vont être gérées mais non à cause du phénomène de *Big data*. Cependant, des problèmes liés aux mégas-données pourraient survenir dans le futur. L'intelligence artificielle utilisée pour des systèmes de police prédictive, pour analyser et essayer de prédire des comportements criminels, est une situation différente et problématique. C'est une situation où les données sont collectées et traitées en masse pour que

l'algorithme fasse son travail. Là, il y a un réel risque que les données de personnes qui n'ont rien à faire avec une enquête policière, soient utilisées et que cette utilisation ait certaines conséquences négatives pour ces personnes. Dans la police en Europe, l'intelligence artificielle n'est pas vraiment encore utilisée mais dans une certaine mesure on y arrive. J'espère et je pense que notre législateur et notre gouvernement vont se rendre compte du risque que cela représente et qu'ils vont installer suffisamment de mesures de contrôle et de protection ainsi que des unités spécifiques indépendantes pour gérer cette intelligence artificielle. Un autre problème lié à la collecte de données massives, pourrait être les *hackings*. À l'heure actuelle, cette masse de données est entre de bonnes mains, entre les mains de la police mais si demain les serveurs de la police se font *hacker* ou si dans cinq ans notre gouvernement change et que ces données se retrouvent entre de mauvaises mains, cela pourrait avoir des conséquences néfastes.

Encore une fois, je ne pense pas qu'on arrivera à un système de surveillance en masse et d'analyser de données en masse, comme en Chine, mais il y aura certaines technologies qui vont être utilisées. La Ligue des droits de l'Homme a un rôle à jouer ; elle devrait mettre en garder et informer les politiques du risque que représente cette nouvelle technologie. J'espère que cela deviendra un débat sociétal.

En conclusion, parait-il réaliste ou utopique de concilier le recueil massif de données à caractère personnel avec leur protection ?

Pieter-Jan De Grave : C'est réaliste. Tout au long de cet entretien j'ai essayé de faire passer le message qu'en soi, traiter des données en masse ce n'est pas un problème, tant que nous respectons certaines garanties. Si nous continuons à traiter ces données uniquement pour des raisons techniques et qu'une fois les données de la cible détectées, les données non pertinentes sont jetées, alors je pense qu'il n'est pas trop difficile de concilier les deux. Je n'ai pas encore rencontré de problèmes en lien avec la collecte et le traitement de données en masse car les enquêteurs veulent le plus rapidement possible cibler la personne en lien avec leur affaire et se « débarrasser » du reste des données. Je suis conscient que dans l'opinion publique, la collecte et le traitement des données en masse ne sont pas très bien perçus, mais selon moi le traitement en masse est peut-être l'un des plus petits problèmes auxquels nous sommes confrontés.

Bibliographie

I. Législation

Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, *J.O.C.E.*, L 281, 23 novembre 1995.

Acte du Conseil du 26 juillet 1995 portant établissement de la convention sur la base de l'article K.3 du traité sur l'Union européenne portant création d'un Office européen de police (convention Europol), *J.O.U.E.*, C 316, 27 novembre 1995.

Décision 2009/371/JAI du Conseil du 6 avril 2009 portant création de l'Office européen de police (Europol), *J.O.U.E.*, L 121, 15 mai 2009.

Le programme de Stockholm – une Europe ouverte et sûre qui sert et protège les citoyens, *J.O.U.E.*, C 115/1, 4 mai 2010.

Charte des droits fondamentaux de l'Union européenne, *J.O.U.E.*, C 326/391, 26 octobre 2012.

Traité sur le fonctionnement de l'Union européenne, *J.O.U.E.*, C 326/47, 26 octobre 2012.

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 119/1, 4 mai 2016.

Directive (UE) 2016/680 de 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.*, L 119/89, 4 mai 2016.

Exposé des motifs du Conseil: Position (UE) no 8/2016 du Conseil en première lecture en vue de l'adoption du règlement du Parlement européen et du Conseil relatif à l'Agence de l'Union européenne pour la coopération des services répressifs (Europol) et remplaçant et abrogeant les décisions 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI et 2009/968/JAI du Conseil, *J.O.U.E.*, C 169/60, 11 mai 2016.

Règlement (UE) 2016/794 du Parlement européen et du Conseil du 11 mai 2016 relatif à l'Agence de l'Union européenne pour la coopération des services répressifs (Europol) et remplaçant et abrogeant les décisions du Conseil 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI et 2009/968/JAI, *J.O.U.E.*, L 135, 24 mai 2016.

Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) n° 45/2001 et la décision n° 1247/2002/CE, *J.O.U.E.*, L 295/39, 21 novembre 2018.

II. Tavaux parlementaires

Proposition de règlement du Parlement européen et du Conseil relatif à l'Agence de l'Union européenne pour la coopération et la formation des services répressifs (Europol) et abrogeant les décisions 2009/371/JAI et 2005/681/JAI, COM (2013) 173 final, Bruxelles, 27 mars 2013.

Document de travail des services de la Commission : résumé de l'analyse d'impact relative à l'adaptation du cadre juridique de l'Office européen de police au traité de Lisbonne, SWD (2013) 99 final part. 1, Bruxelles, 27 mars 2013.

Communication de la Commission au Parlement européen et au Conseil du 6 avril 2016 au sujet des systèmes d'information plus robustes et plus intelligents au service des frontières et de la sécurité, COM (2016) 205 final, Bruxelles, 6 avril 2016.

Note du Conseil de l'Union européenne, « Europol's cooperation with strategic partners: strengths and possible inefficiencies in cooperation with Private Parties », 10494/19, Bruxelles, 4 juillet 2019.

Conseil de l'Union européenne, Conclusions du Conseil sur la coopération entre Europol et les parties privées, 14745/19, Bruxelles, 2 décembre 2019.

Conseil de l'Union européenne, Manuel sur l'échange d'informations en matière répressive, 5825/20, Bruxelles, 2 décembre 2020.

Proposition de règlement du Parlement européen et du Conseil modifiant le règlement (UE) 2016/794 en ce qui concerne la coopération d'Europol avec les parties privées, le traitement de données à caractère personnel par Europol à l'appui d'enquêtes pénales et le rôle d'Europol en matière de recherche et d'innovation, COM (2020) 796 final, Bruxelles, 9 décembre 2020.

III. Jurisprudence

C.J.U.E., arrêt du 6 novembre 2003, *Lindqvist*, aff. C-101/01, EU:C:2003:596.

C.E.D.H., arrêt du 4 décembre 2008, *S. et Marper c. Royaume-Uni*, requêtes 30562/04 et 30566/04.

C.J.U.E., arrêt du 16 décembre 2008, *Tietosuojavaltuutettu c. Satakunnan Markkinapörssi Oy, Satamedia Oy*, aff. C-73/07, EU:C:2008:727.

C.J.U.E., arrête du 26 juin 2010, *Commission européenne c. The Bavarian Lager*, aff. C-28/08, EU:C:2010:378.

C.J.U.E., arrêt du 20 décembre 2017, *Peter Nowak c. Data Protection Commissionner*, aff. C-434/16, EU:C:2017:994.

C.J.U.E., arrêt du 16 juillet 2020, *Data Protection Commissioner c. Facebook Ireland Limited et Maximillian Schrems*, aff. C-311/18, ECLI:EU:C:2020:559.

C.J.U.E., arrêt du 6 octobre 2020, *Privacy International*, aff. C-623/17, ECLI:EU:C:2020:790.

C.J.U.E., arrêt du 6 octobre 2020, *La Quadrature du Net e.a.*, aff. jointes C-511/18, C-512/18 et C-520/18, ECLI:EU:C:2020:791.

IV. Doctrine

AMICI, V., « Europol et la nouvelle décision du Conseil : entre opportunités et contraintes », *R.D.U.E.*, 2010/1.

BENSOUSSAN, A., « Chapitre 2. - Principes » *in Règlement européen sur la protection des données* (sous la dir. de A. BENSOUSSAN), 2e édition, Bruxelles, Bruylant, 2017.

BERTHELET, P., « Europol à l'épreuve du secret. Dépassement du modèle intergouvernemental, respect de l'État de droit et accroissement du contrôle démocratique », *OpenEdition*, 2019.

BERTHELET, P., « Europol face au défi des « méga-données » - L'évolution tendancielle d'une coopération policière européenne « guidée par le renseignement » », *R.D.U.E.*, 2019/2.

BILLET, C., « Le transfert de données à caractère personnel aux États tiers : l'évolution de la protection par l'UE » *in Droits et souveraineté numérique en Europe* (sous la dir. de A. BLANDIN), 1ère édition, Bruxelles, Bruylant, 2016.

BROEDERS, D., SCHRIJVERS, E., VAN DER SLOOT, B., VAN BRAKEL, R., de HOOG, J. et HIRSCH BALLIN, E., « Big Data and security policies: Towards a framework for regulating the phases of analytics and use of Big Data », *Computer Law & Security Review*, vol. 33, 2017.

DAVID, E., « Chapitre VI - La coopération judiciaire et pénale en matière d'enquête et d'instruction » in *Éléments de droit pénal international et européen* (sous la dir. de E. DAVID), 2e édition, Bruxelles, Bruylant, 2018.

DELFORGE, A., « Comment (ré)concilier RGPD et big data ? », *R.D.T.I.*, 2018/1.

DE MONTJOYE, Y.-A., RADAELLI, L., SINGH, V.K. et PENTLAND, A., « Identity and privacy. Unique in the shopping mall: on the reidentifiability of credit card metadata », *Science*, vol. 347, n° 6221, 2015.

DE TERWANGNE, C., « Chapitre 2. - Hypothèses de licéité des traitements » *in Le règlement général sur la protection des données (RGPD/GDPR)* (sous la dir. de C. DE TERWANGNE et K. ROSIER), 1ére édition, Bruxelles, Larcier, 2018.

DE TERWANGNE, C., « Chapitre 9. - Internet et la protection de la vie privée et des données à caractère personnel » *in L'Europe des droits de l'homme à l'heure d'Internet* (sous la dir. de C. DE TERWANGNE et Q. VAN ENIS), 1e édition, Bruxelles, Bruylant, 2019.

DREWER, D. et MILADINOVA, V., « The BIG DATA Challenge: Impact and opportunity of large quantities of information under the Europol Regulation », *Computer Law & Security Review*, vol. 33, 2017.

FLORE, D., *Droit pénal européen : les enjeux d'une justice pénale européenne*, 2e éd., Bruxelles, Larcier, 2014.

MARQUENIE, T., « The Police and Criminal Justice Authorities Directive: Data protection standards and impact on the legal framework », *Computer Law & Security Review*, vol. 33, 2017.

MARTIJN, M. et WIJNBERG, R., « Nee, je hebt wél iets te verbergen », *de Correspondent*, 2013.

MICHEL, A., « Le traçage comportemental des internautes sur les réseaux sociaux : l'affaire des « cookies Facebook », véritable saga judiciaire ? », *R.D.T.I.*, 2019/1.

POULLET, Y., « Avant-propos. Le RGPD – une volonté de bien faire : certes ! … mais appropriée ? » in *Le règlement général sur la protection des données (RGPD/GDPR)* (sous la dir. de C. DE TERWANGNE et K. ROSIER), 1ère édition, Bruxelles, Larcier, 2018.

ROUX-DEMARE, F.-X., « L'inaboutissement des mécanismes de coopération opérationnelle » *in Coopération opérationnelle en droit pénal de l'Union européenne* (sous la dir. de C. BILLET et A. TURMO), 1e édition, Bruxelles, Bruylant, 2020.

ROJSZCZAK, M. « The uncertain future of data retention laws in the EU: Is a legislative reset possible? », *Computer Law & Security Review*, vol. 41, 2021.

SNOWDEN, E., *Permanent Record*, New York City, Metropolitan books, 2019.

TAMBOU, O., « Chapitre 1. - Champ d'application matériel du droit européen de la protection des données à caractère personnel » *in Manuel de droit européen de la protection des données à caractère personnel* (sous la dir. de J.-B. AUBY), Bruxelles, Bruylant, 2020.

TÜRK, A. et PIAZZA, P., « La difficile quête d'un équilibre entre impératifs de sécurité publique et protection de la vie privée », *Cultures & Conflits*, n°76, 2009.

WRR, « Big Data in een vrije en veilige samenleving », *Amsterdam University Press*, 2016.

V. Rapports

Rapport sur la proposition de règlement sur la proposition de règlement du Parlement européen et du Conseil 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 (règlement général sur la protection des données), COM(2012)0011, C7-0025/2012, 21 novembre 2013.

Rapport d'information fait au nom de la commission des affaires européennes sur Europol et Eurojust : perspectives d'avenir, n° 477, Sénat sess. ord, 17 avril 2014.

Rapport de la Commission: les règles de l'UE en matière de protection des données donnent aux citoyens les moyens d'agir et sont adaptées à l'ère du numérique, Bruxelles, 24 juin 2020.

European Data Protection Supervisor, EDPS Decision on the own initiative inquiry on Europol's big data challenge, C 2019-0370, Bruxelles, 18 septembre 2020.

Europol Action Plan addressing the risks raised in the European Data Protection Supervisor (EDPS) Decision on 'Europol's Big Data challenge', doc. 1131384, La Haye, 17 novembre 2020.

Avis du CEPD sur la proposition de modification du règlement Europol, Avis 4/2021, 8 mars 2021.

Résumé de l'avis du contrôleur européen de la protection des données sur la proposition de modification du règlement Europol, *J.O.U.E.*, C 143/6, 23 avril 2021.

Position du CCBE sur la proposition de règlement modifiant le règlement (UE) 2016/794 en ce qui concerne la coopération d'Europol avec les parties privées, le traitement de données à caractère personnel par Europol à l'appui d'enquêtes pénales et le rôle d'Europol en matière de recherche et d'innovation, 6 mai 2021.

European Data Protection Supervisor, Remarks at the LIBE meeting on the follow-up to the EDPS admonishment Europol, 16 juin 2021.

VI. Liens Internet

Europol Work Programme 2016, mis en ligne le 3 février 2016, disponible sur https://www.europol.europa.eu/publications-documents/europol-work-programme-2016 (date de la dernière consultation : 12 juin 2020).

AEDH, Europol : une fuite de données massive qui révèle où sont les risques, disponible sur : https://www.ldh-france.org/europol-fuite-donnees-massive-revele-les-risques/ (date de la dernière consultation : 02 août 2021).

Europol, *Internet Organised Crime Threat Assessment (IOCTA)*, mis en ligne le 18 septembre 2018, disponible sur https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018 (date de la dernière consultation : 3 juillet 2020).

Colloque du 20 janvier 2020 organisé par le CEDAG (Centre de Droit des Affaires et de Gestion de la Faculté de Droit, d'économie et de gestion de l'Université de Paris), *Le droit européen des données personnelles : à la recherche d'une cohérence (1ère partie)*, disponible sur : https://www.youtube.com/watch?v=kmdzeLkPCNA (date de la dernière consultation : 30 juin 2021).

Europol, *Pandemic profiteering how criminals exploit the COVID-19 crisis*, mis en ligne le 27 mars 2020, disponible sur : https://www.europol.europa.eu/publications-documents/pandemic-profiteering-how-criminals-exploit-covid-19-crisis (date de la dernière consultation : 22 juin 2021).

Europol, *Europol in brief, year of 2019*, mis en ligne le 16 décembre 2020, disponible sur https://www.europol.europa.eu/activities-services/main-reports/europol-in-brief-2019 (date de la dernière consultation : 10 juin 2021).

Sénat, *Proposition de règlement du Parlement européen et du Conseil modifiant le règlement (UE) 2016/794 en ce qui concerne la coopération d'Europol avec les parties privées, le traitement de données à caractère personnel par Europol à l'appui d'enquêtes pénales et le rôle d'Europol en matière de recherche et d'innovation*, disponible sur :

https://www.senat.fr/ue/pac/EUR000006727.html?fbclid=IwAR3xJog8FcgTRty55PSFpJA7TxnIey4wx_gK-khd5_yibr96SMdi5Q1m-0U (date de la dernière consultation : 24 juin 2021).

LOUVAIN-LA-NEUVE | BRUXELLES | MONS | TOURNAI | CHARLEROI | NAMUR
Place Montesquieu, 2 bte L2.07.01, 1348 Louvain-la-Neuve, Belgique | **www.uclouvain.be/drt**