Doctrine

L'AFFAIRE DU « CASIER BIS » : LE DROIT À LA PROTECTION DES DONNÉES PERSONNELLES À L'ÉPREUVE DE LA PRATIQUE INSTITUTIONNELLE

CATHERINE WARIN
DOCTEURE EN DROIT
AVOCATE À LA COUR

Juin 2019. « Le Luxembourg tient une nouvelle affaire politique. Le fichier central de la police, baptisé *"casier bis"* ou "casier secret", se trouve tout à coup sur le devant de la scène, alors que ce dernier existe depuis… 1992. Aucun ministre, aucun député, aucun avocat, aucun magistrat ni aucun citoyen ne s'est jusqu'à présent plaint de l'existence de ce fichier, qui comprend donc tous les procès-verbaux dressés par la police, peu importe si les faits ont mené à une condamnation ou pas. »[1]

L'élément déclencheur du scandale : une procédure de recrutement pour un poste de référendaire-bibliothécaire auprès de la magistrature en 2018. Un candidat est confronté lors de son entretien à ce qu'il décrit comme un « casier judiciaire fantôme », un dossier retraçant des faits remontant à près de huit ans pour certains, comme la participation à une bagarre et l'outrage à une personne dépositaire de l'autorité publique. Or ces faits, consignés dans des procès-verbaux de police à l'époque, n'ont donné lieu à aucune condamnation et n'ont jamais été inscrits au casier judiciaire de l'intéressé. Comment de tels éléments ont-ils pu refaire surface lors d'un entretien d'embauche ?

Quelques mois après l'entretien (et le refus de la candidature de l'intéressé), la sphère politique s'empare de l'affaire. Le 17 avril 2019, le député Laurent Mosar introduit une question parlementaire pour demander des précisions sur le « *casier bis* »[2]. Le lendemain, le journaliste Guy Kaiser publie sur son *blog* un billet au titre anxiogène : « *Lëtzebuerg a KGB-Zäiten ?* »[3]. S'ensuivent plusieurs mois de polémique : la Chambre des députés se fait le théâtre de débats houleux[4], le gouvernement fait face à une cinquantaine de questions parlementaires appelant notamment le ministre de la Sécurité intérieure à s'expliquer, le Parquet général se fend d'une conférence de presse, la Commission nationale pour la protection des données et l'Inspection générale de la police sont sollicitées pour enquêter et rendent des avis montrant l'institution policière sous un jour peu favorable[5].

L'affaire du *casier bis* illustre à merveille la complexité des rapports entre progrès technologique, évolution normative, et pratique institutionnelle. Si l'opinion publique peut aujourd'hui s'étonner, voire s'indigner, de la collecte et de l'utilisation de données personnelles sur des bases légales discutables par la police et par la justice, c'est sans doute parce que nous commençons à ressentir les effets de la construction d'un cadre juridique européen et national exigeant en matière de protection des données personnelles, y compris dans le champ d'action des services de police et des autorités judiciaires (I). La mise en œuvre de cette législation exigeante a permis non seulement de mettre en lumière les pratiques liées au *casier bis*, mais aussi de faire évoluer ces pratiques (II). Néanmoins, des zones d'ombre persistent, démontrant la nécessité de développer une véritable culture des données personnelles au sein de nos institutions (III).

I. LA RECHERCHE D'UN ÉQUILIBRE ENTRE DROIT À LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL ET EFFICACITÉ DES FORCES DE L'ORDRE

La protection de la vie privée fait partie intégrante de l'ordre constitutionnel luxembourgeois depuis la naissance du Grand-Duché ; cette protection a été renforcée par le législateur au fil du temps et a connu une expansion importante sous l'influence du droit européen (A). Les activités des services de police et des autorités judiciaires n'échappent pas à cette tendance, ainsi qu'en attestent la jurisprudence de la Cour européenne des droits de l'homme (B) et le cadre conçu par le législateur de l'Union (C).

1. D. Marques, « En roue libre », *Le Quotidien,* 21 juin 2019.
2. Question parlementaire n° 640 de M. le Député Laurent Mosar du 17 avril 2019, Banque de données similaire au casier judiciaire.
3. G. Kaiser, « Lëtzebuerg a KGB-Zäiten ? », 18 avril 2019, https://guykaiser.lu/letzebuerg-a-kgb-zaiten/.
4. D. Marques, « Casiers bis : coup d'éclat à la Chambre », *Le Quotidien*, 9 juillet 2019.
5. L. Schmit, « Was wir über die Datenbanken von Polizei und Justiz wissen », *Reporter*, 26 juin 2019 ; L. Schmit, « CNPD sieht Grundrechte gefährdet », *Reporter*, 19 septembre 2019 ; L. Caregari, « Fichiers de la police : aucune sensibilité », *Woxx*, 6 décembre 2019.

A. La tradition luxembourgeoise de protection de la vie privée modernisée par l'exigence européenne de protection des données à caractère personnel

Le Luxembourg peut faire valoir une certaine tradition de protection de la vie privée[6], puisque des aspects essentiels de cette protection, comme l'inviolabilité du domicile et le secret des correspondances, figuraient déjà dans la Constitution du 9 juillet 1848[7]. Par la suite, le constituant et le législateur ont continué à renforcer la protection de la sphère privée contre des ingérences non justifiées des autorités publiques ; la Constitution du 17 octobre 1868 a ainsi étendu le secret postal (protégé par l'article 28) à celui des télégrammes. Depuis la loi du 11 août 1982 concernant la protection de la vie privée, ce secret couvre toutes les télécommunications[8].

À partir des années 1970, la protection légale de la vie privée, tenant compte de l'évolution des moyens technologiques[9], a été étendue à toutes les branches du droit. En matière pénale, le Code de procédure pénale impose désormais un cadre très strict définissant les circonstances et les conditions dans lesquelles les autorités peuvent procéder à des repérages et des écoutes téléphoniques[10]. Le même Code contient depuis 2006 des dispositions réglant le recours aux empreintes génétiques (ADN) en vue de l'identification d'une personne dans le cadre des enquêtes préliminaires et des instructions préparatoires[11]. En droit du travail, la surveillance (notamment la vidéosurveillance) des salariés sur le lieu de travail est strictement encadrée par le livre II, titre VI, du Code du travail. La procédure administrative non contentieuse a aussi intégré l'exigence de protection de la vie privée, puisque l'administré a droit à la communication de son dossier et peut demander l'enlèvement de toute pièce étrangère à l'objet du dossier qui est de nature à lui causer préjudice. En outre, l'administration peut refuser la communication d'informations susceptibles de porter atteinte à l'intimité de la vie privée d'autres personnes[12]. Enfin, la révision constitutionnelle du 29 mars 2007 a introduit l'article 11 (3) de la Constitution, suivant lequel « L'État garantit la protection de la vie privée, sauf les exceptions fixées par la loi. »

En parallèle, le Luxembourg a bénéficié de la construction progressive du cadre européen de protection de la vie privée. La Convention européenne des droits de l'homme protège ainsi le droit à la protection de la vie privée en son article 8, dont est d'ailleurs directement inspiré l'article 11 (3) de la Constitution précité[13]. Le Conseil de l'Europe a aussi été à l'origine de la Convention de 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, approuvée au Luxembourg en 1987[14].

Le droit de l'Union européenne a également connu des développements importants en la matière.

Le tout premier arrêt de la Cour de justice de ce que l'on appelait alors les Communautés européennes en matière de droits fondamentaux, l'arrêt *Stauder*, portait précisément sur le droit à la protection de la vie privée[15]. En 1995, la directive 95/46 a imposé aux États membres de prendre des mesures allant dans le sens de la Convention de 1981[16]. Bien plus tard, le traité de Lisbonne a posé les fondements d'une protection renforcée de la protection des données à caractère personnel : le droit à la protection de la vie privée est désormais consacré à l'article 7 de la Charte des droits fondamentaux de l'Union européenne, juste avant le droit à la protection des données personnelles (article 8). S'y ajoute l'article 16 du Traité sur le fonctionnement de l'Union européenne, qui habilite le législateur européen à fixer les règles en la matière.

Cette disposition a fourni la base pour l'adoption du fameux règlement général sur la protection des données (RGPD), entré en vigueur en mai 2018[17]. Ce règlement s'inscrit dans la démarche affichée des institutions européennes de donner aux individus le contrôle de leurs données personnelles et de promouvoir une véritable culture de la protection des données[18]. L'entrée en vigueur de ce

6. Pour un historique détaillé, *cf. Le Conseil d'État, gardien de la Constitution et des droits et libertés fondamentaux,* Luxembourg, Conseil d'État du Grand-Duché du Luxembourg, septembre 2007, pp. 125-129.
7. *Cf.* art. 16 et 29 de la Constitution du 9 juillet 1848, devenus les articles 15 et 28 de la Constitution du 27 novembre 1856.
8. Loi du 11 août 1982 concernant la protection de la vie privée, *Mém. A/ J.O.G.D.L.*, n° 86.
9. *Le Conseil d'État, gardien de la Constitution et des droits et libertés fondamentaux, op. cit.*, pp. 20-23.
10. Loi du 26 novembre 1982 portant introduction au Code d'instruction criminelle des articles 88-1, 88-2, 88-3 et 88-4 (écoutes téléphoniques), *Mém. A/J.O.G.D.L.*, n° 98.
11. La Loi du 25 août 2006 relative aux procédures d'identification par empreintes génétiques en matière pénale et portant modification du Code d'instruction criminelle, *Mém. A/J.O.G.D.L.*, n° 163, a créé les articles 48-3 à 48-9 du Code de procédure pénale et modifié ou complété plusieurs autres dispositions de ce Code.
12. Article 11, 2e alinéa, et article 13 du Règlement grand-ducal du 8 juin 1979 relatif à la procédure à suivre par les administrations relevant de l'État et des communes (*Mém. A/J.O.G.D.L.*, n° 54).
13. *Le Conseil d'État, gardien de la Constitution et des droits et libertés fondamentaux, op. cit.*, p. 23.
14. Loi du 19 novembre 1987 portant a) approbation de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, faite à Strasbourg, le 28 janvier 1981 ; b) modification de la loi du 31 mars 1979 réglementant l'utilisation des données nominatives dans les traitements informatiques, *Mém. A/J.O.G.D.L.*, n° 94.
15. CJUE, arrêt *Stauder c. Stadt Ulm*, 12 novembre 1969, C-26/69, EU:C:1969:57.
16. 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.*, L 281, 23 novembre 1995, pp. 31-50.
17. Règlement 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et abrogeant la directive 95/46/CE (règlement général sur la protection des données), *J.O.U.E.*, L 119/1, 4 mai 2016.
18. COM(2012) 9 final, 21 janvier 2012 ; European Data Protection Supervisor, « Promoting a new culture of data protection », 2019.

règlement a permis la montée en puissance des autorités nationales chargées de la protection des données, notamment la Commission nationale pour la protection des données (CNPD), dont les rapports et prises de position trouvent régulièrement un écho dans les médias et qui a d'ailleurs rendu un avis très détaillé sur le *casier bis*[19]. Nous avons tous pu constater par ailleurs les implications pratiques quotidiennes de la mise en œuvre du RGPD – qu'il s'agisse des obligations de mise en conformité dans les milieux professionnels[20] ou des messages d'information affichés au gré de notre navigation sur internet. Le cadre législatif et institutionnel posé par le législateur européen a ainsi un impact tangible à l'échelle nationale, locale et même individuelle.

De plus, la Cour de justice de l'Union européenne s'assure du respect du droit à la protection des données, qu'elle combine souvent avec le droit à la protection de la vie privée[21]. On citera notamment les très médiatisés arrêts *Schrems* concernant le stockage de données par un acteur privé (Facebook pour ne pas le nommer) et la possibilité de transferts internationaux de données personnelles[22]. En particulier, dans le premier volet de la saga *Schrems*, la Cour a établi que l'accès généralisé par des autorités publiques (qu'elles soient européennes ou non) au contenu de communications électroniques viole l'essence même du droit fondamental au respect de la vie privée tel que protégé par l'article 7 de la Charte[23]. La résonance médiatique des arrêts de la Cour de justice de l'Union européenne a sans doute contribué à sensibiliser l'opinion publique à la problématique de la protection des données à caractère personnel.

B. La protection des données à caractère personnel traitées dans le cadre spécifique des activités des services de police et de justice : la jurisprudence de la Cour européenne des droits de l'homme

La collecte et le traitement des données personnelles par les forces de l'ordre soulèvent des questions spécifiques, notamment celle de l'équilibre entre sécurité publique (voire intérêt national) et protection de la vie privée. Cette tension a nourri une jurisprudence riche et intéressante de la part de la Cour européenne des droits de l'homme notamment. Dans l'affaire *Segerstedt-Wiberg*[24] en particulier, les demandeurs savaient que des données les concernant étaient conservées par les services de sécurité et de renseignement suédois, mais ils n'y avaient pas accès. La Cour a insisté sur l'importance d'un cadre légal strict encadrant la collecte et le stockage de l'information par les services de sécurité et sur la nécessité de prévoir des procédures permettant à un individu de contester le refus d'accès aux informations détenues.

En matière de police à proprement parler, la Cour européenne des droits de l'homme s'est notamment prononcée sur les mesures de surveillance que pouvait prendre la section antiterroriste de la police en vertu de la législation hongroise : l'arrêt *Szabo et Vissy c. Hongrie*[25] a établi que la législation en question n'était pas assortie de garanties suffisamment précises, effectives et complètes en ce qui concerne la prise, l'exécution et la réparation éventuelle des mesures de surveillance, de sorte qu'il y avait violation de l'article 8 de la Convention européenne des droits de l'homme. En outre, dans son arrêt *Gaughran*[26], la Cour a examiné la conservation sans limitation de durée des données personnelles (profil ADN, empreintes digitales et photographie) d'un homme reconnu coupable de conduite en état d'ivresse en Irlande du Nord, et dont la condamnation avait été rayée de son casier judiciaire à l'expiration du délai prévu par la loi. La Cour a constaté une violation du droit à la vie privée, non pas à cause de la durée de la détention des données, mais à cause de l'absence de certaines garanties. Les autorités avaient décidé de conserver sans limitation de durée les données personnelles du requérant, sans tenir compte de la gravité de l'infraction commise, sans justifier de la nécessité de conserver les données en question sans limitation de durée, et sans lui offrir une réelle possibilité de réexamen. Par conséquent, la conservation des données personnelles du requérant ne traduisait pas un juste équilibre entre les intérêts publics et privés concurrents.

C. Les exigences croissantes du législateur de l'Union pour la protection des données à caractère personnel en matière pénale

Le législateur de l'Union a également pris la mesure des spécificités de la collecte et du traitement de données par les autorités de police et les autorités judiciaires. L'envergure européenne de cette thématique s'était déjà concrétisée avec le développement du Système d'information Schengen, instauré par la Convention d'applica-

19. Avis de la Commission nationale pour la protection des données relatif au fichier central de la police grand-ducale au regard de la législation sur la protection des données, Délibération n° 45/2019 du 13 septembre 2019 (ci-après « Avis de la CNPD relatif au fichier central »).
20. Prenant note des enjeux pour les entreprises, la Chambre des métiers a mis en ligne une page dédiée à l'accompagnement de celles-ci dans la transition : « La culture de la donnée », 24 juin 2020, disponible sur https://www.cdm.lu/news/fiche/newsnew/news/la-culture-de-la-donnee (consulté le 24 août 2020).
21. CJUE, arrêt *Volker and Markus Schecke and Eifert*, 9 novembre 2010, C-92/09 et C-93/09, EU:C :2010:662, point 85 ; CJUE, arrêt *Digital Rights Ireland*, 8 avril 2014, EU:C:2014:238. H. Hofmann, « A critical assessment of the relation of information freedom and the protection of personal data in today's EU law / Les données personnelles des Européens dans le monde digital (14 mars 2017) », *Actes de la section des Sciences morales et politiques de l'Institut grand-ducal*, 2018, vol. XXI, p. 22.
22. CJUE, arrêt *Schrems*, 6 octobre 2015, C-362/14, EU:C:2015:650, point 94 ; CJUE, arrêt *Schrems*, 25 janvier 2018, C-498/16, EU:C:2018:37 ; CJUE, arrêt *Facebook Ireland et Schrems*, 16 juillet 2020, C-311/18, EU:C:2020:559. H. Hofmann, « A critical assessment of the relation of information freedom and the protection of personal data in today's EU law / Les données personnelles des Européens dans le monde digital », *op. cit.*, p. 25.
23. CJUE, arrêt *Schrems*, 6 octobre 2015, C-362/14, EU:C:2015:650, point 94.
24. Cour EDH, arrêt *Segerstedt-Wiberg et autres c. Suède*, 6 juin 2006, n° 62332/00.
25. Cour EDH, arrêt *Szabó et Vissy c. Hongrie*, 12 janvier 2016, n° 37138/14.
26. Cour EDH, arrêt *Gaughran c. Royaume-Uni*, 13 février 2020, n° 45245/15.

tion des accords de Schengen du 19 juin 1990 comme un système de recherche de personnes et d'objets afin de compenser la suppression des contrôles aux frontières intérieures entre les États signataires de ces accords. La deuxième « génération » de ce système est encore en vigueur aujourd'hui[27]. En 2008, une décision-cadre[28] portant sur les échanges transfrontaliers de données entre les autorités de police et de justice a été adoptée. La directive « Police-Justice »[29], préparée en parallèle du RGPD, a succédé récemment à cette décision-cadre. Ce texte ambitieux, adapté aux défis de la numérisation, établit des règles relatives 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. Toutes ces dispositions ont fait l'objet d'une transposition par la loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale[30]. Nous présentons ci-dessous quelques dispositions de la directive parmi les plus pertinentes pour notre propos[31], et leurs équivalents dans la loi luxembourgeoise[32].

En ce qui concerne le champ d'application de la directive Police-Justice, notons d'abord que l'article 3, sous 1), nous donne une définition d'une « donnée à caractère personnel » : « toute information se rapportant à une personne physique identifiée ou identifiable [...] ; est réputée être une "personne physique identifiable" une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale[33] ». Le champ d'application de la directive est plus précisément défini en son article premier. Le champ personnel couvre les traitements de données à caractère personnel mis en œuvre par une « autorité compétente » : principalement les autorités judiciaires et la police, mais aussi les autres autorités répressives et les organismes et entités à qui le droit d'un État membre confie l'exercice de l'autorité publique et de prérogatives de puissance publique aux fins de mettre en œuvre un traitement relevant de la directive (par exemple, les services internes de sécurité dans les transports, etc.). Le champ matériel est celui de la « matière pénale », soit les activités menées pour la prévention et la détection des infractions pénales, d'enquêtes et de poursuites en la matière, ou encore d'exécution de sanctions pénales[34]. L'article premier de la loi du 1er août 2018 en matière pénale y ajoute le traitement des données personnelles en matière de sécurité nationale. Cet article est donc très important, car il permet de délimiter le champ d'application de la loi du 1er août 2018 en matière pénale, par rapport à celui du RGPD.

La directive pose d'ailleurs plusieurs exigences très similaires à celles établies par le RGPD. Le chapitre IV de la directive prévoit ainsi le principe de la protection des données dès la conception et la protection des données par défaut (*privacy by design and by default*, article 19 de la loi du 1er août 2018 en matière pénale, correspondant à l'article 20 de la directive). En d'autres termes, la directive exige que la protection de la vie privée soit intégrée dans les nouvelles applications technologiques dès leur conception et que chaque entité traitant des données personnelles garantisse, *par défaut,* le plus haut niveau possible de protection des données. Le législateur impose également des précautions encadrant le recours à des sous-traitants pour les activités de traitement de données (articles 21 et 22 de la loi correspondant aux articles 22 et 23 de la directive). La loi impose aussi la notification à la personne concernée d'une violation de données à caractère personnel (article 30 de la loi et article 31 de la directive), et la désignation d'un délégué à la protection des données (article 31 de la loi et article 32 de la directive) pour chaque responsable de traitement. Au Luxembourg, le Parquet général a ainsi désigné son « DPO » (*data protection officer*), et la police grand-ducale a fait de même[35]. En outre, le chapitre VI de la directive exige comme le RGPD que des autorités de contrôle indépendantes soient mises en place suivant des règles précises, ce qu'a fait le Grand-Duché en désignant à l'article 39 de la loi du 1er août 2018 la Commission nationale pour la protection des données comme l'autorité de contrôle compétente pour contrôler et vérifier le respect de cette loi, et en créant à l'article 40 une « Autorité de contrôle judiciaire » chargée de contrôler la protection des données traitées par les juridictions.

27. Décision 2007/533/JAI du Conseil du 12 juin 2007 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II), *J.O.*, L 205, 7 août 2007, pp. 63-84 et Règlement du Parlement européen et du Conseil 1987/2006 du 20 décembre 2006 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SISII), *J.O.*, L 381, 28 décembre 2006, pp. 4-23.
28. Décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale, *J.O.*, L 350, 30 décembre 2008, pp. 60–71 (abrogée).
29. Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, *J.O.*, L 119, 4 mai 2016, pp. 89-131.
30. *Mém. A/J.O.G.D.L.*, n° 689 (ci-après « la Loi du 1er août 2018 en matière pénale »).
31. Pour une description détaillée et un commentaire approfondi de la directive Police-Justice, *cf.* J. Sajfert et T. Quintel, « Data protection directive (EU) 2016/680 for police and criminal justice authorities », *GDPR Commentary*, M. Cole et F. Boehm (dir.), Edward Elgar Publishing, 2019.
32. Pour un descriptif et une analyse détaillée de cette loi, *cf.* Avis de la CNPD relatif au fichier central, pp. 7 et s.
33. Cette définition est la même que celle donnée par l'article 4, sous 1), du RGPD.
34. Les traitements mis en œuvre pour les activités de sûreté de l'État et de défense nationale ne sont pas régis par le droit de l'Union européenne.
35. Ceux-ci sont joignables respectivement à l'adresse dpo@justice.etat.lu et à l'adresse dpo@police.etat.lu, comme l'indiquent les sites internet des institutions en question.

D'autres dispositions sont spécifiques à la matière pénale et donnent aux États membres une latitude supérieure à celle qu'ils ont pour la mise en œuvre du RGPD. L'article 4(1)(c) de la directive Police-Justice, repris tel quel par l'article (3)(1)(c) de la loi du 1er août 2018 en matière pénale, prévoit que les données personnelles collectées dans ce cadre soient « adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont traitées ». Ce principe donne aux services de police et aux autorités judiciaires une marge de manœuvre plus grande que celle prévue par le RGPD, dont l'article 5(1)(c) exige que les données collectées soient limitées au strict nécessaire.

De même, l'article 5 de la directive donne aux États membres une marge de manœuvre dans la fixation des délais appropriés pour l'effacement des données à caractère personnel et la vérification de la nécessité de conserver ces données. Or, la transposition de cette disposition dans l'article 4 de la loi du 1er août 2018 a été jugée inadéquate par la CNPD. Celle-ci, consultée sur le projet de loi, avait en effet désapprouvé le choix du législateur national de confier la fixation des délais de conservation au responsable du traitement (donc au directeur général de la police pour ce qui est des données traitées par la police)[36]. Le législateur n'ayant pas tenu compte de cette objection, le directeur général de la police a fixé un délai de dix ans de conservation (aligné sur les délais de prescription prévus dans le Code de procédure pénale), après quoi les données sont archivées, et finalement effacées soixante ans après leur premier enregistrement. Soixante ans : en somme, toute une vie. La CNPD considère que cette durée est disproportionnée au regard des finalités poursuivies et regrette que des règles procédurales n'aient pas été fixées pour assurer le respect des délais de conservation et leur proportionnalité, comme l'exige pourtant la directive[37]. Cette insuffisance est révélatrice d'une différence de pratique importante entre le RGPD qui s'impose aux États membres sans marge de manœuvre, et la liberté laissée au législateur national par la directive Police-Justice et qui se traduit ici par une protection lacunaire des données à caractère personnel collectées par la police.

La directive Police-Justice impose en outre plusieurs distinctions et processus afin de structurer les bases de données des forces de l'ordre. L'article 6, transposé par l'article 5 de la loi, distingue entre plusieurs catégories de personnes concernées : personnes suspectées d'avoir commis une infraction pénale, personnes reconnues coupables d'une telle infraction, victimes d'une infraction pénale et enfin tiers, par exemple personnes susceptibles d'être entendues comme témoins. Cette distinction répond aux exigences posées par la Cour européenne des droits de l'homme, qui a jugé que traiter de façon indifférenciée les données relatives à des personnes déjà condamnées et celles relatives à des personnes n'ayant été reconnues coupables d'aucune infraction faisait naître un « risque de stigmatisation » de ces dernières et portait atteinte à leur droit à la présomption d'innocence[38].

L'article 7 de la directive, transposé par l'article 6 de la loi, impose ensuite la vérification de la *qualité* des données à caractère personnel, ce qui implique en particulier que les données à caractère personnel « fondées sur des faits » soient, « dans la mesure du possible, distinguées de celles fondées sur des appréciations personnelles ». Cette seconde catégorie correspond par exemple aux appréciations ou impressions que les policiers peuvent consigner lorsqu'ils rédigent un procès-verbal : le législateur cherche à s'assurer que de telles données ne seront pas assimilées à des faits vérifiés lorsqu'elles seront exploitées ultérieurement. Ceci implique également que les autorités compétentes vérifient la qualité des données à caractère personnel avant toute transmission et que les autorités destinataires aient les informations nécessaires pour en évaluer la qualité. Citons enfin l'obligation de journalisation inscrite à l'article 25 de la directive et transposée par l'article 24 de la loi : la tenue de journaux où sont inscrites les opérations de traitement effectuées doit permettre de contrôler la légalité de l'usage des bases de données.

Ainsi, la directive impose une cartographie des bases de données utilisées par les forces de l'ordre, et trace les voies pour y naviguer : il incombe ensuite aux concepteurs, mainteneurs et utilisateurs de ces bases de se conformer à ces exigences.

La loi du 1er août 2018 en matière pénale, conformément à la directive, traite encore des transferts internationaux de données personnelles entre autorités de police et de justice : ce volet n'est pas directement pertinent pour éclairer l'affaire des « *casiers bis* », si ce n'est pour souligner l'importance de la légalité et de la qualité des données personnelles collectées au Luxembourg, sachant que ces données sont susceptibles d'être transférées en Europe, voire au-delà. Une législation efficace est particulièrement importante pour les données à caractère sensible qui sont collectées en matière pénale, de telles données pouvant être manipulées, combinées avec d'autres données, voire échangées avec d'autres autorités.

Enfin, le contrôle du respect de la législation sur la protection des données à caractère personnel par les forces de l'ordre et les services de la justice est assuré par des autorités dont l'existence et les fonctions sont prévues par la directive Police-Justice, relayée par les dispositions de droit luxembourgeois. Il s'agit d'abord de la CNPD, qui est compétente pour contrôler et vérifier le respect

36. Avis de la Commission nationale pour la protection des données relatif au projet de loi n° 7168 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale et portant modification de certaines lois, Délibération n° 1049/2017 du 28 décembre 2017, pp. 1-3.

37. Avis de la CNPD relatif au fichier central, pp. 8-9.

38. Cour EDH, arrêt *S. et Marper c. Royaume-Uni*, 4 décembre 2008, nos 30562/04 et 30 566/04, point 122.

non seulement du RGPD, mais aussi de la loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale[39]. En outre, en ce qui concerne les opérations de traitement de données à caractère personnel effectuées par les juridictions, l'article 40 de la loi du 1er août 2018 a créé une Autorité de contrôle judiciaire qui « conseille la Chambre des députés, le Gouvernement et d'autres institutions et organismes au sujet des mesures législatives et administratives relatives à la protection des droits et libertés des personnes physiques à l'égard du traitement »[40].

La législation sur le traitement des données personnelles en matière pénale est ainsi le fruit d'un exercice d'équilibre délicat entre, d'une part, les exigences de sécurité nationale et d'ordre public et, d'autre part, le droit de chaque personne physique à la protection de ses données personnelles[41]. Une protection effective de ce droit individuel impose une exigence de transparence, puisque, pour exercer ce droit, il est nécessaire de savoir qui est responsable de la collecte et du traitement, quelles données ont été collectées et utilisées, et quelles voies de recours existent. Par conséquent, paradoxalement peut-être, le droit à la vie privée appelle le développement d'une culture de la transparence et de règles favorisant cette transparence[42].

II. LE *CASIER BIS* À LA LUMIÈRE DES PRINCIPES DE PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL : L'AJUSTEMENT NÉCESSAIRE ET PROGRESSIF DE LA PRATIQUE

L'agitation médiatique et politique autour du *casier bis* a eu l'effet intéressant de pousser les autorités à rendre des comptes publiquement. Les informations données dans un premier temps par le Parquet général et par le gouvernement, puis les enquêtes de la CNPD, de l'IGP et de l'Autorité de contrôle judiciaire permettent ainsi de cerner plus précisément la nature du fameux *casier bis* (A) et de mettre en lumière la nécessité de faire évoluer la pratique vers une meilleure conformité aux principes que nous avons résumés ci-dessus, en particulier en ce qui concerne la durée de conservation des données personnelles (B) et le contrôle et la traçabilité des accès à ces données (C).

A. Du scandale du casier bis aux éclaircissements sur le « fichier central » et la « Jucha »

Lors de sa conférence de presse du 28 juin 2019, le Parquet général a tenté de clarifier ce qu'était, ou plutôt ce que n'était pas le *casier bis*. Concrètement, Mme le Procureur général d'État a commencé par indiquer lors de sa conférence de presse que l'ensemble des fichiers mis en cause ne constitue pas un casier judiciaire électronique, mais que le système indique, pour chaque affaire à laquelle est attribuée un numéro, les documents versés par les différents acteurs et les noms des parties prenantes. « Il n'existe aucun dossier au nom de Pierre ou Paul », nous dit encore M. le Procureur général d'État adjoint[43]. La déléguée à la protection des données de la police tient le même discours en réponse à des individus cherchant à savoir ce que contient le *casier bis* à leur sujet : « Ce fichier ne contient *pas* de fiches par personne », lit-on dans une lettre adressée à Me Gaston Vogel[44]. Or, ce n'est évidemment pas tant la forme sous laquelle les données personnelles sont conservées qui a choqué l'opinion publique, mais bien le fait même que ces données soient conservées et puissent être consultées, compilées et utilisées. À l'âge de l'informatique en réseau, et même de l'informatique en nuage, l'accessibilité des données stockées par les autorités augmente de façon exponentielle, de même que la vulnérabilité de ces données. Le progrès technologique nous empêche de nous contenter d'une définition immuable, vite désuète, du « dossier » ou du « casier », et impose aux juristes en particulier d'ajuster leurs concepts pour s'approprier les nouvelles réalités du terrain[45].

L'enquête réalisée par la CNPD nous apprend que le fichier central de la police « existe depuis que les services de police ont commencé à rédiger des procès-verbaux et rapports afin de les transmettre aux autorités judiciaires conformément à la loi, alors qu'il fallait disposer d'un outil permettant d'assurer le suivi adéquat de ces procès-verbaux et rapports. Le fichier central est opérationnel sous forme informatisée depuis 2005. » Ce fichier central rassemble « les procès-verbaux et les rapports de la

39. Article 4, respectivement alinéa 1 et alinéa 3, de la Loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données (*Mém. A/J.O.G.D.L.*, n° 686).
40. Le règlement interne de cette autorité vient d'entrer en vigueur (Règlement interne de l'autorité de contrôle de la protection des données judiciaires, *Mém. B/J.O.G.D.L.*, n° 3003, 2020).
41. Cette tension entre impératif d'efficacité des services publics et protection de la vie privée n'est bien sûr pas spécifique à la matière pénale : un parallèle intéressant peut être dressé avec les difficultés rencontrées par l'administration des services de secours, laquelle se voit limitée dans ses missions par l'interdiction de la géolocalisation « Luxembourg's emergency services : between security and data protection », *Luxembourg Times,* 13 décembre 2016, https://luxtimes.lu/archives/3929-luxembourg-s-emergency-services-between-security-and-data-protection.
42. *Cf.*, en ce sens, H. Hofmann, « A critical assessment of the relation of information freedom and the protection of personal data in today's EU law / Les données personnelles des Européens dans le monde digital », *op. cit.*, pp. 35-36.
43. C. Frati, « Il n'y a pas de "casier judiciaire bis" », *Paperjam*, 28 juin 2019.
44. Lettre du 7 août 2019 publiée par le destinataire sur son site internet, disponible sur http://www.vogel.lu/wp-content/uploads/2019/08/Fichier-Police-Me-Vogel-13.08.19-SD-1.pdf.
45. N. Balabanian, « The Neutrality of Technology: A Critique of Assumptions », *Critical Approaches to Information Technology in Librarianship: Foundations and Applications*, J. Buschman, Westport (Connecticut), Greenwood Press, 1993, p. 17 ; M. L. Jones, « Does Technology Drive Law ? The Dilemma of Technological Exceptionalism in Cyberlaw », *Brussels Privacy Hub Working Paper*, juillet 2017, vol. 3, n° 10, p. 8.

police »[46]. La CNPD nous apprend encore que ce fichier est scindé en deux parties, l'une « signalétique » renseignant des métadonnées de types noms, prénoms, lieu et date de naissance, nationalité, adresse et numéro de matricule, éventuellement date du décès ; l'autre « documentaire » comprenant les procès-verbaux et rapports, organisés en dossiers dont chacun correspond à une personne. Plus précisément, « un numéro de dossier unique est attribué à chaque personne concernée. Cette même personne peut être reliée à plusieurs documents différents en fonction du nombre d'affaires dans lesquelles elle est impliquée et qui ont donné lieu à un procès-verbal ou à un rapport ». Même s'il faut donc effectuer une recherche manuelle pour retrouver les documents mentionnant une personne[47], il n'est finalement pas si difficile de reconstituer un « dossier au nom de Pierre ou Paul » dont le Parquet général niait farouchement l'existence. Au moment de l'enquête de la CNPD, celle-ci a pu constater que le système contenait plus de 500 000 fichiers, dont environ les deux tiers étaient archivés (c'est-à-dire accessibles seulement via une procédure particulière et un déplacement supplémentaire pour physiquement accéder au fichier souhaité)[48].

Si le projecteur a surtout été braqué sur le fichier central de la police, le fonctionnement de la la chaîne pénale de la justice, dite « Jucha », a aussi été mis en cause, ce qui a poussé l'Autorité de contrôle judiciaire à s'autosaisir pour évaluer la légalité de cette application utilisée depuis 2009 par l'administration judiciaire pour gérer la « chaîne pénale », c'est-à-dire le processus qui commence avec la communication d'une infraction au ministère public par la police et s'achève avec la décision définitive sur l'action publique. Ainsi que l'enquête de l'Autorité de contrôle judiciaire permet de le confirmer, la nature de cette application rappelle par bien des aspects le fichier central de la police, encore que la numérisation des documents répertoriés dans la Jucha semble moins avancée. Néanmoins, comme l'indique l'Autorité de contrôle judiciaire, la tendance est à la dématérialisation de l'ensemble des fichiers[49], ce qui ne fait qu'accentuer le parallèle que l'on peut tracer entre les deux applications. La pertinence d'un tel parallèle est également renforcée par la porosité entre le fichier central de la police et la Jucha, la circulation des informations du premier vers la seconde étant illustrée par le déroulement de l'entretien d'embauche du candidat référendaire, et surtout confirmée par l'Autorité de contrôle judiciaire dans son récent avis[50].

S'il n'y a pas de *casier bis* au sens restrictif autour duquel les autorités judiciaires ont tenté de circonscrire le débat, il existe bien au sein des services de la police et de la justice, des applications informatiques permettant la collecte et la consultation d'une abondante quantité de données à caractère personnel. Ceci n'est ni surprenant ni choquant et, en ce qui concerne la Jucha, sa base légale remonte à un règlement grand-ducal de 1988[51] et réside désormais dans la loi du 1er août 2018. Pour ce qui est du fichier central, le Parquet général s'est attaché à préciser que les bases de données de la police ont une existence légale depuis 1979 (loi sur la protection des données), à l'exception d'une période de trois ans au début des années 1990[52]. Le gouvernement a ajouté le 17 juin 2019, en réponse à une question parlementaire[53], que depuis l'entrée en vigueur de la loi du 1er août 2018 « la question de la base légale de tous les fichiers de la police ne se pose plus ». Il est vrai que la loi du 1er août 2018 fournit une base légale pour le stockage de données à caractère personnel par la police, dans la limite des attributions conférées à celle-ci par la loi du 18 juillet 2018 sur la police grand-ducale[54], dont l'article 43 liste en outre les traitements de données personnelles auxquels ont accès les officiers de police. L'affirmation lapidaire du gouvernement est pourtant loin de clore le débat quant à la légalité des fichiers mis en cause, et surtout de l'utilisation qui en est faite.

Sans entrer dans une critique détaillée des pratiques policière et judiciaire à la lumière de la législation antérieure à 2018, il y a lieu au minimum d'émettre un doute sur la légalité de la conservation et de l'utilisation des données collectées *avant* l'entrée en vigueur de la loi du 1er août 2018 et surtout avant les efforts de mise en conformité qui ont suivi l'éclatement du scandale du *casier bis*. En ce qui concerne les pratiques contemporaines, sur la base des avis produits par les autorités compétentes, nous mentionnerons ici deux éléments qui nous paraissent particulièrement importants au regard des grands principes concrétisés par la législation relative à la protection des données à caractère personnel : la problématique de la durée de conservation des données, et les

46. Avis de la CNPD relatif au fichier central, p. 2.
47. Ce qu'explique aussi la déléguée à la protection des données de la police dans la lettre précitée adressée à Me Vogel : « la Police doit rechercher manuellement si votre nom figure sur un procès-verbal ou rapport intégré dans le Fichier central, respectivement s'il figure dans les autres fichiers de la police. Dans l'affirmative, il faut à nouveau vérifier par des recherches manuelles quelles données personnelles sont traitées par rapport à une personne concernée. »
48. Avis de la CNPD relatif au fichier central, pp. 2-3.
49. Avis de l'Autorité de contrôle judiciaire, p. 2.
50. Celle-ci souligne « la diversité des sources qui alimentent l'application Jucha », les systèmes de la police comptant parmi ces sources. Avis de l'Autorité de contrôle judiciaire, p. 12.
51. Règlement grand-ducal du 13 juin 1988 autorisant la création et l'exploitation d'une banque de données nominatives, dite chaîne pénale, au parquet de Luxembourg (*Mém. A/J.O.G.D.L.*, n° 34).
52. Nous croyons comprendre que le règlement grand-ducal du 2 octobre 1992 relatif à la création et à l'exploitation d'une banque de données nominatives de police général (*Mém. A/J.O.G.D.L.*, n° 74) est censé avoir comblé ce vide juridique.
53. Question parlementaire n° 752 de M. le Député Laurent Mosar et de M. le Député Gilles Roth du 4 juin 2019, Existence de casiers judiciaires *bis* ; Réponse commune de M. le Ministre de la Sécurité intérieure François Bausch et de M. le Ministre de la Justice Félix Braz du 17 juin 2019 à la question parlementaire n° 752 du 4 juin 2019 des honorables députés Laurent Mosar et Gilles Roth.
54. Loi du 18 juillet 2018 sur la police grand-ducale, *Mém. A/J.O.G.D.L.*, n° 621.

enjeux autour du contrôle et de la traçabilité des accès à ces données.

B. Un premier axe d'amélioration clairement identifié : la durée de conservation des données

En ce qui concerne la durée de conservation des données contenues dans les fichiers de la police et de la justice, rappelons que la CNPD s'est déjà prononcée par rapport au fichier central et qu'elle considère que ni l'autorité désignée par la loi pour fixer cette durée (la police, c'est-à-dire le responsable du traitement lui-même) ni la durée effectivement fixée (dix ans avant archivage, puis encore cinquante ans avant effacement, sans distinction entre les différentes informations consignées) ne correspondent aux exigences posées par le droit de l'Union, notamment en termes de proportionnalité[55]. La problématique est illustrée concrètement par l'exemple de Me Vogel qui s'interroge sur « le fait que des papillons de stationnement, de longue date réglés » continuent à figurer au fichier central alors même qu'« aucun de ces papillons n'a eu de suite judiciaire »[56]. Il nous paraît en effet légitime de mettre en doute la conformité d'une telle pratique à la jurisprudence *Gaughran*[57] et à l'exigence d'un juste équilibre entre les intérêts publics et privés, lorsque les données relatives à des contraventions mineures sont susceptibles d'être conservées par les autorités pendant des décennies[58].

Les conclusions de l'Autorité de contrôle judiciaire concernant la Jucha sont un peu moins sévères. L'Autorité reconnaît qu'une des finalités de la Jucha est de permettre aux procureurs d'apprécier l'opportunité des poursuites, ce qu'ils font notamment en retraçant l'historique d'une personne, y compris les affaires pénales qui n'ont pas abouti à un procès pénal ou celles qui ont occasionné un non-lieu ou une relaxe. L'Autorité de contrôle judiciaire met en doute la proportionnalité de cette utilisation des données dans la mesure où les données conservées permettent de remonter très loin dans le temps. Mais elle souligne que, dans l'attente d'une intervention du législateur, un ajustement a commencé : la dernière mise à jour de l'application limite ainsi la visibilité de l'existence même des affaires « archivées » depuis plus de cinq ans[59]. Un autre effort du même ordre est en cours, pour les affaires liées à la coopération internationale en matière pénale et judiciaire, dont la pratique d'archivage n'était pas alignée sur la pratique pour les autres affaires, à savoir un archivage après trois ans, mais cet alignement serait « en train d'être instauré en pratique »[60]. L'Autorité de contrôle constate donc un retard dans l'ajustement des pratiques, mais souligne aussi que cet ajustement est bien amorcé, ce qui est sans nul doute un développement positif en termes de protection des données à caractère personnel. Néanmoins, on peut regretter que l'Autorité ne conteste pas la légitimité de principe de la possibilité, pour le ministère public, de remonter sur des décennies pour retracer les affaires concernant une personne, y compris les affaires n'ayant même pas donné lieu à des poursuites[61] : il n'est pourtant pas si évident que ces données doivent ou puissent être conservées sur une durée indéfinie[62].

Au-delà des efforts actuellement mis en œuvre par les responsables des traitements – services de police comme de justice –, l'Autorité de contrôle judiciaire indique que « les débats actuels autour des traitements de données mis en œuvre par la police grand-ducale, autour du "fichier central", au sein de la Chambre des députés, et notamment les échanges avec le ministère de la Sécurité intérieure et le ministère de la Justice, semblent faire émerger un consensus qu'il revient au législateur de fixer les durées de conservation ou les règles procédurales pour la vérification des délais de conservation, en suivant dorénavant l'avis de la CNPD sur cette question »[63]. Par conséquent, une évolution intéressante devrait se produire avec l'intervention du législateur sur la durée de conservation des données. Étant donné la position exprimée par la CNPD, cette évolution devrait aller dans le sens de durées plus limitées et sans doute plus différenciées selon le type de données conservées.

C. Un deuxième axe d'amélioration clairement identifié : le contrôle et la traçabilité des accès

L'autre piste incontournable d'amélioration des pratiques actuelles concerne le contrôle et la traçabilité de l'accès aux données personnelles par les fonctionnaires de la police et de la justice. La CNPD pour le fichier central, comme l'Autorité de contrôle judiciaire pour la Jucha, se sont à juste titre montrées soucieuses du respect des obligations légales sur ce terrain. La CNPD a en effet déploré que l'accès aux informations contenues dans le fichier central soit si peu contrôlé et si peu tra-

55. Cf. *supra*, p. x et avis de la CNPD relatif au fichier central, p. 8.
56. G. Vogel, Lettre au directeur de la Police du 13 août 2019, disponible sur http://www.vogel.lu/lettre-au-directeur-de-la-police-casier-bis/.
57. Cour EDH, arrêt *Gaughran c. Royaume-Uni*, 13 février 2020, n° 45245/15.
58. À titre de comparaison, le fichier français de traitement d'antécédents judiciaires (TAJ), employé par la police et la gendarmerie en application des articles 230-6 à 230-11 du Code de procédure pénale, prévoit des durées de conservation différentes selon que les données sont relatives à des personnes mises en cause majeures, mineures, ou à des victimes. La durée standard pour les mises en cause majeures est de vingt ans, mais de cinq ans pour certaines délits et contraventions, et une durée dérogatoire de quarante ans est prévue pour certains crimes et délits (soi bien en-deçà des soixante années de conservation au sein du fichier central). Les données concernant les victimes sont conservées au maximum quinze ans.
59. Avis de l'Autorité de contrôle judiciaire, p. 17.
60. Avis de l'Autorité de contrôle judiciaire, p. 18.
61. Avis de l'Autorité de contrôle judiciaire, p. 18.
62. *Cf.* S. Braum, « Ju-Cha-Datenbank / Juraprofessor Braum : Die Diskussion ist um einiges komplexer als bisher dargestellet », *Tageblatt*, 16 septembre 2020.
63. Avis de l'Autorité de contrôle judiciaire, p. 15.

çable. Il est vrai que l'on pouvait déjà s'étonner que le gouvernement ait eu tant de mal à évaluer (ou à communiquer ?) le nombre de personnes ayant un tel accès : après un premier chiffre de 630 avancé dans les premiers jours du scandale, la réponse du gouvernement à la question parlementaire indique plutôt près de 2000 personnes, ce que confirme la CNPD[64]. Suivant celle-ci, la nécessité des accès accordés n'est pas établie, puisque « l'accès au fichier central est accordé d'office à chaque nouvel agent ou officier de police judiciaire », la seule justification étant « qu'il pourra être amené à travailler avec cet outil »[65].

Sur ce point, le rapport de l'IGP complète utilement celui de la CNPD en précisant que lorsqu'un policier est muté à un nouveau poste, il garde les accès aux fichiers de son poste d'avant, même lorsqu'il n'en a pas forcément besoin[66]. À cela s'ajoute un problème de traçabilité des consultations du fichier : les agents et officiers de police n'ont pas accès à distance au fichier central, cet accès n'étant possible qu'à partir d'un poste de travail hébergé dans les locaux sécurisés de la police. Par conséquent, quand les équipes sur le terrain ont besoin d'une consultation (par exemple, lors d'un contrôle de police administrative), ils contactent leurs collègues du siège pour faire la recherche : or, « les recherches effectuées sont loguées sous le nom du policier qui a réalisé la recherche et non pas celui qui a effectué la demande au préalable. Le retraçage des appels des policiers sur le terrain n'est pour le moment pas réalisé »[67]. En outre, la journalisation inscrite à l'article 25 de la directive et transposée par l'article 24 de la loi du 1er août 2018 (tenue de journaux où sont inscrites les opérations de traitement effectuées) n'a pas été systématisée, de sorte que la traçabilité de la consultation des données personnelles n'est pas assurée[68]. Les pratiques en termes d'accès aux données stockées (quantité et qualité des personnes qui l'exercent et modalités de l'accès) s'avèrent ainsi profondément problématiques à la lumière de la législation en vigueur. En bout de ligne, ces illégalités mettent en péril l'objectif poursuivi par les dispositions en question, à savoir permettre un contrôle de la légalité des traitements de données. L'IGP semble consciente de la gravité du problème, puisqu'elle a proposé que les accès soient non seulement liés à la fonction, mais aussi remis à zéro en cas de changement de fonction[69].

Il semble que, sur la question des accès, l'institution judiciaire soit en meilleure voie de se conformer aux exigences légales, ou peut-être le contraste est-il simplement dû au décalage temporel entre les enquêtes de la CNPD et de l'IGP sur le fichier central de la police, dont les conclusions ont été rendues publiques en 2019, et l'enquête sur la Jucha, diligentée plus tardivement par l'Autorité de contrôle judiciaire. Toujours est-il que cette dernière indique que des réunions de travail sont en cours afin de redéfinir les catégories d'accès (casier judiciaire, parquet, cabinet d'instruction, tribunaux d'arrondissement de Luxembourg et de Diekirch, greffes, etc.) et de définir les profils d'accès aux différentes permissions de la Jucha, et que ce processus devrait être achevé « sous peu ». Sur la journalisation, le bilan est également plutôt positif, puisque le retraçage des accès est déjà faisable ; l'Autorité recommande cependant « d'adapter ce mécanisme en prévoyant la saisie obligatoire du motif de consultation et/ou de modification d'une notice » dans la Jucha[70]. De telles adaptations paraissent tout à fait pertinentes pour prévenir, sinon sanctionner des consultations tout à fait abusives, et qui ne sont pas qu'hypothétiques, ainsi qu'en atteste le cas bien réel d'une greffière mise en cause pour avoir consulté la Jucha à des fins purement personnelles[71]. Heureusement, la tendance, pour la Jucha comme pour le fichier central, est à un affinement des modalités de contrôle et de traçage des accès.

Le débat public suscité par l'affaire du *casier bis* a indubitablement contribué à une mise en question des pratiques de la police et de la justice en matière de données personnelles et, surtout, les enquêtes diligentées sur ces pratiques ont permis d'éclairer certaines non-conformités majeures à la législation applicable, ce qui est bien sûr un préalable à la rectification de ces non-conformités. Ainsi, des problèmes ont été clairement identifiés en ce qui concerne la durée de conservation des données collectées et les modalités de consultation de ces données, et des recommandations précises ont été formulées et semblent en bonne voie d'être mises en œuvre. Sur d'autres points, malheureusement, un manque de transparence est encore à déplorer.

III. DES ZONES D'OMBRE PERSISTANTES RÉVÉLATRICES D'UNE CULTURE DES DONNÉES PERSONNELLES ENCORE INSUFFISAMMENT DÉVELOPPÉE

Si les enquêtes diligentées à la suite de l'éclatement du scandale du *casier bis* ont permis d'actionner un processus bénéfique de mise en conformité, une certaine opacité sur les fichiers de la police fait encore obstacle à la bonne et complète application du droit à la protection des données personnelles (A). Le problème est amplifié par un certain flou quant aux voies de recours censées permettre de

64. 1840 personnes précisément au 30 juillet 2019. Avis de la CNPD relatif au fichier central, p. 4.
65. Avis de la CNPD relatif au fichier central, p. 3.
66. L. Caregari, « Fichiers de la police : aucune sensibilité », *Woxx*, 6 décembre 2019.
67. Avis de la CNPD relatif au fichier central, pp. 3-4.
68. Avis de la CNPD relatif au fichier central, p. 19.
69. M. Fick, « La police des polices épingle les lacunes des fichiers », *Luxemburger Wort*, 4 décembre 2019.
70. Avis de l'Autorité de contrôle judiciaire sur la Jucha, p. 21.
71. CA (Ch.c.), 4 juin 2019, ord. n° 507/19.

faire valoir ce droit (B). Pour assurer pleinement la protection des données à caractère personnel à l'avenir, il paraît nécessaire d'encourager le développement d'une véritable culture des données personnelles au sein des services de la police et de la justice (C).

A. Des zones d'ombre demeurent sur le fonctionnement du fichier central, au détriment du droit à la protection des données personnelles

Le fichier central de la police a beau avoir fait l'objet de deux enquêtes (celle de la CNPD, puis celle de l'IGP), force est de constater que l'exercice de transparence auquel se sont adonnées les autorités connaît des limites, de sorte qu'il est impossible de faire un bilan exhaustif du fonctionnement du système et donc d'estimer la conformité de ce système à la législation en vigueur, ou même la probabilité d'une mise en conformité prochaine.

Tout d'abord, on ne peut que s'étonner d'apprendre que la CNPD, lors de son enquête, n'a eu qu'un accès limité à certaines informations dont elle aurait pourtant eu besoin pour procéder à une analyse approfondie, comme ses attributions le lui permettent. Ainsi, la CNPD a pu constater que les droits d'accès, de rectification et d'effacement de certaines données tombant dans le champ d'application du RGPD[72] étaient susceptibles de limitations pour les besoins des services de police ; or, la CNPD indique qu'elle « ne dispose pas d'informations » quant à ces limitations, « et ne peut donc pas se prononcer quant à la proportionnalité des procédures appliquées »[73].

Ensuite, une mauvaise surprise attend le citoyen qui chercherait à étudier en détail les résultats de l'enquête de l'IGP. Le rapport de cette dernière n'est tout simplement pas accessible au public[74]. Il faut se contenter des éléments qui ont été communiqués lors de la conférence de presse. Or, ces éléments complètent le rapport de la CNPD sur des points très intéressants. L'IGP a ainsi constaté une certaine porosité entre différents fichiers, comme entre les données de la police administrative et les fichiers relevant du pénal. On apprend encore par la presse que la banque de données du matériel ADN fonctionne de façon problématique : les profils ADN sont effacés après la clôture du dossier dans le cadre duquel ils ont été établis, mais les noms des personnes y restent toujours inscrits. L'IGP a aussi constaté que les fichiers de la police ne sont pas correctement comptabilisés : la police en comptait soixante-trois, l'IGP en a découvert trois supplémentaires, ce qui porterait leur total à soixante-six. Il est étonnant de constater que l'IGP a pu accéder à des informations auxquelles la CNPD ne semble pas avoir eu accès, tandis que celle-ci est l'autorité légalement compétente pour contrôler le respect par la police de la loi du 1er août 2018 en matière pénale. En outre, les éléments problématiques que nous venons de mentionner sont ceux que l'IGP a bien voulu dévoiler : sans possibilité de consulter le rapport complet, comment peut-on exclure que d'autres problèmes aient également été identifiés lors de l'enquête ?

Sur d'autres points, la gêne vient plutôt de l'absence de communication sur les modalités de mise en conformité, par exemple en ce qui concerne la vérification de la qualité des données conservées dans le fichier central de la police. Il n'existe pas de procédure claire pour systématiser une telle vérification (qui pourrait consister en un retour des autorités judiciaires aux services de police pour mettre à jour, voire supprimer des données à la suite d'un acquittement). Une telle procédure serait en cours d'élaboration à la mi-2019, suivant les informations obtenues par la CNPD[75]. Pourtant, le rapport de l'IGP quelques mois plus tard déplore toujours la présence dans les fichiers de « données douces » : appréciations personnelles des policiers, rumeurs, constats dont la fiabilité est d'autant plus douteuse qu'aucune méthode de contrôle de la qualité des données n'a encore été mise en place[76]. Ainsi, les informations sont extrêmement limitées quant aux intentions de la police face à une lacune pourtant clairement identifiée et que la loi impose de combler.

Une incertitude similaire concerne la structuration des bases de données de la police. En effet, si l'article 5 de la loi du 1er août 2018 prévoit, à l'image de l'article 6 de la directive, que l'on puisse distinguer de façon structurée entre la qualité des personnes concernées par les données (condamnés, suspects, victimes, tiers, etc.), la CNPD a constaté que cette distinction n'était techniquement pas possible dans le système actuel de la police[77]. Une telle lacune technique pose un sérieux problème non seulement au regard de l'obligation expressément posée par l'article 5 de la loi du 1er août 2018 et par la directive, mais encore par rapport au droit de la Convention européenne des droits de l'homme, puisque la distinction posée par les dispositions précitées répond aux préoccupations de la Cour quant aux risques de stigmatisation qu'occasionnerait un traitement indifférencié des données relatives à des personnes de qualités différentes au regard de la procédure pénale[78].

72. Droits protégés respectivement par les articles 12(3), 14 et 15(4) du RGPD.
73. Avis de la CNPD relatif au fichier central, p. 16.
74. Nous avons tenté d'obtenir le rapport en contactant l'IGP via le formulaire disponible sur son site internet. Après une première demande restée sans réponse, une deuxième demande a permis d'obtenir la réponse suivante de la part de l'Inspecteur général adjoint de la police : « Je suis au regret de vous informer que le rapport auquel vous faites allusion n'est pas accessible au public ».
75. Avis de la CNPD relatif au fichier central, pp. 10-11.
76. L. Caregari, « Fichiers de la police : aucune sensibilité », *Woxx*, 6 décembre 2019.
77. Avis de la CNPD relatif au fichier central, p. 10.
78. Cour EDH, arrêt *S. et Marper c. Royaume-Uni*, 4 décembre 2008, n° 30562/04 et 30 566/04, point 122. (*cf. supra*, I.B).

Ces deux problèmes sont amplifiés par la circulation des données entre les services de police et les institutions judiciaires. Certes, l'Autorité de contrôle judiciaire constate que la Jucha « semble respecter » l'exigence de distinction des données suivant la qualité des personnes concernées[79]. Mais si des données mal triées ou non vérifiées peuvent effectivement être transmises au ministère public par les services de police, la structuration correcte de la Jucha ne suffira pas à rectifier les erreurs ou les illégalités potentiellement contenues dans les informations émanant de la police.

Le manque de transparence sur la façon dont les données à caractère personnel sont collectées et utilisées porte donc effectivement atteinte au respect du droit de chaque individu à la protection de ses données.

B. La difficile mise en œuvre des droits individuels octroyés par la législation sur la protection des données

Ce problème trouve son prolongement dans une certaine confusion quant aux modalités d'exercice des droits découlant de la législation sur la protection des données. Certes, la police grand-ducale s'est attachée à répondre aux multiples demandes d'individus souhaitant connaître le contenu de leur *casier bis*. Mais nous venons de voir que les droits d'accès, de rectification et d'effacement de certaines données tombant dans le champ d'application du RGPD[80] étaient susceptibles de limitations pour les besoins des services de police, sans que ces limitations soient clairement justifiées ni leur proportionnalité établie[81]. Nous ne pouvons donc pas exclure que certaines personnes demeurent dans l'ignorance de l'existence de données les concernant et auxquelles elles devraient légalement avoir accès. Dans ces conditions, il serait difficilement imaginable de formuler une réclamation dont l'objet serait, justement, inconnu.

En outre, les réclamations qui concernent les données exploitées par les juridictions doivent être adressées à l'Autorité de contrôle judiciaire. Or, l'article 16.3 de la loi du 1er août 2018 en matière pénale est formulé de façon assez étrange : « Lorsque le droit visé au paragraphe 1er est exercé, l'autorité de contrôle compétente informe au moins la personne concernée du fait qu'elle a procédé à toutes les vérifications nécessaires ou à un examen. L'autorité de contrôle informe également la personne concernée de son droit de former un recours juridictionnel. » L'Autorité a donc une obligation d'informer la personne concernée des actions qu'elle a menées, mais cet article ne l'oblige pas directement à agir d'une façon déterminée. Le règlement de l'Autorité de contrôle judiciaire[82] n'est guère plus explicite sur les attributions de l'Autorité dans le traitement de ces réclamations. Le dernier alinéa de l'article 7 de ce règlement nous indique que « [d]ans le cadre de l'instruction du recours, l'autorité de contrôle judiciaire peut nommer rapporteur un de ses membres » ; là encore, la disposition est formulée de telle sorte que l'Autorité dispose d'une grande latitude dans sa façon de traiter les réclamations. La contrepartie en est que les particuliers auront bien du mal à déduire de la loi ou du règlement ce qu'ils peuvent attendre de la procédure de réclamation devant l'Autorité de contrôle judiciaire. Ce manque de clarté nous paraît donc nocif pour l'exercice effectif du droit à un recours, et ce, même si les voies de recours juridictionnelles (c'est-à-dire celles qui pourraient être exercées contre une décision concernant une réclamation) sont en revanche clairement déterminées dans la loi[83].

C. Vers le développement d'une culture de la protection des données ?

Au terme de la conférence de presse lors de laquelle l'IGP a présenté les conclusions de son enquête sur le fichier central, l'inspecteur général adjoint a déclaré : « Il faut admettre que la sensibilité à la protection des données n'est pas acquise. Il y a un manque de culture en ce qui concerne le maniement des données sensibles.[84] »

Ce diagnostic nous semble juste et ne s'applique pas qu'aux services de police. Rappelons qu'au moment de l'éclatement du scandale du *casier bis*, le Parquet général a tenté de justifier sa consultation du fameux casier en arguant que les référendaires « sont amenés à consulter des dossiers pénaux, à rédiger des notes et ont accès à des données sensibles », de sorte qu'il serait précisément « scandaleux » de ne pas vérifier leurs antécédents ; pour preuve, le candidat avait justement fait preuve de malhonnêteté en niant avoir eu affaire à la police dans sa jeunesse, ce que démentaient les données contenues dans le fichier central[85]. Pourtant, à la lumière des principes que nous avons exposés ci-dessus, et comme l'avait d'ailleurs affirmé l'avocat de l'intéressé[86], un tel raisonnement est difficilement tenable.

79. Avis de l'Autorité de contrôle judiciaire, p. 13.
80. Droits protégés respectivement par les articles 12(3), 14 et 15(4) du RGPD.
81. Avis de la CNPD relatif au fichier central, p. 16.
82. *Mém. B/J.O.G.D.L.*, n° 3003, 2020.
83. L'article 45, sous 1), de la loi du 1er août 2018 en matière pénale prévoit qu'un recours contre une décision prise par l'Autorité de contrôle judiciaire dans le champ d'application de ladite loi peut être introduit par la personne concernée devant la chambre du conseil de la cour d'appel ; l'article 45, sous 2), prévoit qu'un recours contre une décision prise par la CNPD ou par l'Autorité de contrôle judiciaire dans le champ d'application du RGPD peut être introduit devant le tribunal administratif.
84. Propos de l'inspecteur général adjoint V. Fally rapportés par L. Caregari, « Fichiers de la police : aucune sensibilité », *Woxx*, 6 décembre 2019.
85. C. Frati, « Il n'y a pas de "casier judiciaire bis", *Paperjam*, 28 juin 2019.
86. « Dans l'affaire du casier "le Parquet a fait une erreur" », *Luxemburger Wort*, 17 juillet 2019.

En effet, la collecte et l'utilisation de données personnelles à des fins de ressources humaines par les services de police entre dans le champ du RGPD et non dans celui de la loi du 1er août 2018, dont le champ matériel est celui de la « matière pénale », soit les activités menées pour la prévention et la détection des infractions pénales, d'enquêtes et de poursuites en la matière, ou encore d'exécution de sanctions pénales. Lorsqu'un agent de police manipule des données pour des besoins liés aux ressources humaines de son service, c'est le RGPD qui s'applique[87]. Ce règlement ne permet certainement pas à un comité de recrutement de se renseigner sur un candidat en consultant des données sensibles qui avaient été collectées des années auparavant dans une tout autre finalité[88]. En outre, s'il peut être justifié de consulter les antécédents judiciaires d'un candidat à un poste « sensible », la loi prévoit justement cette possibilité en passant par la consultation du casier judiciaire ; plus précisément, depuis la dernière réforme entrée en vigueur en février 2017, il existe cinq types de casier judiciaire différents avec différentes mentions selon la finalité du bulletin[89]. Les données relatives aux antécédents judiciaires d'une personne transitent ainsi par ce média dont le contenu et les modalités de communication sont strictement encadrés.

Certaines dispositions légales permettent certes aux services qui procèdent au recrutement de certains profils d'employer d'autres méthodes. Pour le recrutement des magistrats, la loi du 7 juin 2012 sur les attachés de justice[90] prévoit en son article 2, paragraphe 2, sous 2, que pour être admis à l'examen-concours d'attaché de justice il faut notamment « jouir des droits civils et politiques et présenter les garanties d'honorabilité requises », la commission de recrutement pouvant « demander des renseignements à ce sujet aux autorités judiciaires et à la police grand-ducale ». L'expression est malheureusement vague, néanmoins nous n'imaginons pas que ceci donne un blanc-seing quant au type d'informations qui seront demandées ou communiquées, puisque les autorités judiciaires sont elles-mêmes tenues par les principes concrétisés dans la loi du 1er août 2018 en matière pénale. On peut d'ailleurs faire un parallèle avec les dispositions relatives à la consultation de données personnelles dans le recrutement des fonctionnaires du cadre de la police. Jusqu'à 2018, un règlement grand-ducal régissait cette question et indiquait que les garanties de moralité requises devaient faire l'objet d'un avis du directeur général de la police[91]. La loi du 18 juillet 2018 sur la police prévoit désormais en son article 58 qu'une « enquête de moralité » soit effectuée « sur ordre du ministre par la police, qui peut consulter les fichiers qui lui sont légalement accessibles et pour autant que cette consultation est pertinente quant à la finalité recherchée ». Ainsi, le législateur a jugé nécessaire de fixer pour le recrutement de catégories bien précises de fonctionnaires, des dispositions dérogatoires du droit commun. En dehors de ces cas de figure, l'exploitation des bases de données de la police et de la justice à des fins de ressources humaines (ou à toute autre fin non prévue par la loi du 1er août 2018 en matière pénale) est tout simplement illégale.

L'ignorance des exigences légales en matière de protection des données à caractère personnel (ou du moins de la traduction pratique de ces exigences) par les effectifs de l'institution judiciaire a d'ailleurs donné lieu à une ordonnance intéressante d'un juge d'instruction en 2019. Une information avait été ouverte concernant une greffière qui avait consulté l'application Jucha pour des raisons personnelles. La fonctionnaire risquait des sanctions pénales pour accès et maintien frauduleux dans tout ou partie d'un système de traitement ou de transmission de données (article 509-1 du Code pénal) et pour violation du secret professionnel et du secret de l'instruction. Or, le juge d'instruction a considéré qu'il ne ressortait pas du dossier répressif que l'intéressée savait « qu'elle n'avait pas le droit de consulter l'application Jucha à des fins privées » ; elle savait seulement qu'elle n'avait pas le droit de communiquer les informations *à l'extérieur* de la juridiction. En outre, son contrat de travail mentionnait « la révélation d'informations couvertes par le secret professionnel à des tiers mais ne (faisait) aucune référence à une consultation de documents/fichiers internes à des fins non professionnelles ». Enfin, lors de son engagement, l'intéressée n'avait signé « aucune clause de confidentialité » qui lui aurait expressément interdit de consulter des documents ou fichiers internes à des fins non professionnelles. Pour ces motifs, le juge d'instruction a décidé de ne pas procéder à l'inculpation[92]. Cette affaire atteste à tout le moins de la nécessité impérieuse d'informer et de former les fonctionnaires aux règles modernes relatives à la protection des données.

Précisément, l'Autorité de contrôle judiciaire indique dans son avis que le principe de la consultation limitée aux besoins du service a été « porté à la connaissance des magistrats et fonctionnaires par le biais d'instructions de service ». Les agents disposant d'un accès à la Jucha ont

87. J. Sajfert et T. Quintel, « Data protection directive (EU) 2016/680 for police and criminal justice authorities », *op. cit.*

88. Suivant l'article 5, paragraphe 1, sous b), du RGPD, les données à caractère personnel doivent être « collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités ».

89. Loi du 23 juillet 2016 portant modification 1) de la loi du 29 mars 2013 relative à l'organisation du casier judiciaire, 2) du Code d'instruction criminelle, 3) du Code pénal, *Mém. A/J.O.G.D.L.*, n° 154.

90. Loi du 7 juin 2012 sur les attachés de justice, *Mém. A/J.O.G.D.L.*, n° 125.

91. Règlement grand-ducal du 27 avril 2007 déterminant 1) les conditions de recrutement, d'instruction et d'avancement du personnel policier ; 2) les conditions d'admission au Service de police judiciaire et au Service de contrôle à l'aéroport [...], *Mém. A/J.O.G.D.L.*, n° 90. Article 2, sous e), pour les candidats au cadre supérieur policier ; article 9, sous e), pour les candidats à la carrière d'inspecteur de police ; article 30, sous g), pour les candidats à la carrière de brigadier de police. De même, l'article 49, sous c), de ce règlement prévoit que le ministre statue sur la candidature au Service de police judiciaire sur la base notamment d'un avis du directeur général de la police. Règlement pris en application de la loi modifiée du 31 mai 1999 portant création d'un corps de police grand-ducale et d'une inspection générale de la police, *Mém. A/J.O.G.D.L.*, n° 87 (abrogée par la loi de 2018).

92. CA (Ch.c.), 4 juin 2019, ord. n° 507/19.

également été informés que « même si un accès est techniquement possible en raison de leur affectation, leur droit d'accès n'est pas pour autant illimité, mais doit être justifié au cas par cas » et enfin qu'« en cas de consultation non justifiée par un besoin de service, l'agent est disciplinairement, voire pénalement, responsable »[93]. Dans le même esprit, l'IGP propose qu'il y ait une formation sur la thématique des données personnelles dès le recrutement des fonctionnaires de la police, puis également une formation continue. On peut donc espérer qu'une sensibilité collective à cette question se développe au sein des institutions et services concernés.

CONCLUSION

« L'évolution technique dépend elle-même de la culture juridique à un moment donné[94] », nous dit Alain Supiot. Il est vrai que le législateur européen a posé des exigences ambitieuses pour la protection des données personnelles collectées en matière pénale. Or, l'affaire du *casier bis* nous montre que ces normes exogènes ont trouvé des relais puissants non seulement dans la législation nationale, mais aussi dans l'opinion publique luxembourgeoise. Aux institutions policière et judiciaire d'adapter leurs pratiques désormais, étant entendu que, comme l'a souligné la CNPD, il ne leur sera pas possible de « se réfugier derrière des contraintes techniques pour justifier une non-conformité. Il incombe [...] au responsable du traitement de prendre toutes les mesures nécessaires pour assurer qu'il soit en mesure de respecter pleinement les droits des personnes concernées »[95]. Nous pouvons espérer que la sensibilité à la protection des données personnelles devienne à terme partie intégrante de la culture des services de police et de justice.

93. Avis de l'Autorité de contrôle judiciaire sur la Jucha, p. 23.
94. A. Supiot, *Homo juridicus. Essai sur la fonction anthropologique du droit*, Paris, Éditions du Seuil, 2005, p. 180.
95. Avis de la CNPD relatif au fichier central, p. 34.