e-legal

Revue de droit et de criminologie
de l'Université libre de Bruxelles

L'effacement des données policières et judiciaires : un parcours du combattant ?

Par Catherine Forget

e-legal, Volume n°6

Pour citer l'article :
Catherine Forget, « L'effacement des données policières et judiciaires : un parcours du combattant ? », *in e-legal, Revue de droit et de criminologie de l'ULB,* Volume n°6, mars 2022.

Adresse de l'article :
https://e-legal.ulb.be/volume-n06/la-peine-ne-s-arrete-pas-a-la-sortie-de-prison/l-effacement-des-donnees-policieres-et-judiciaires-un-parcours-du-combattant

L’inscription d’informations personnelles dans les banques de données policières et judiciaires est source de difficultés pour la réinsertion d’un individu sortant de prison mais aussi pour toute personne dite « connue » des services de police. Outre le fait que le respect des règles relatives aux traitements de données à caractère personnel par les services de police n’est en pratique, pas exempt de critiques, pour pouvoir exercer ses droits, la personne concernée doit s’élancer dans un véritable « parcours du combattant ».

Introduction

§1 S'il est bien connu que le casier judiciaire constitue un obstacle important pour la réinsertion[1], l'inscription d'informations personnelles dans les banques de données policières et judiciaires est également source de nombreuses difficultés pour l'individu sortant de prison et cherchant à retrouver une place au sein de la société. De manière plus large, cette problématique concerne toute personne dite « connue » des services de police dès lors que certaines informations la concernant sont enregistrées dans des banques de données, parfois même sans qu'elle n'en ait connaissance ou qu'elle n'ait jamais fait l'objet de poursuites pénales. Cet enregistrement peut non seulement générer un sentiment d'incompréhension mais également provoquer des conséquences désagréables voire pénibles pour la personne visée. Celle-ci peut effet être contrainte de se soumettre à des contrôles d'identité renforcés à l'aéroport impliquant parfois un interrogatoire, subir des fouilles sans justification, ou encore, être dans l'impossibilité d'obtenir une attestation de sécurité dans le cadre de ses activités professionnelles la privant *de facto* de l'exercice de son métier. Autant d'éléments qui constituent de véritables obstacles à la (ré)insertion. Pourtant, obtenir des renseignements clairs quant à l'origine de ce « fichage » peut s'avérer une véritable gageure.

§2 Comme nous l'examinerons dans le cadre de cette contribution, il existe en effet en Belgique quatre types de banques de données policières opérationnelles[2] : la banque nationale générale (ci-après B.N.G.), les banques de données de base, les banques de données particulières et les banques de données communes. Les règles relatives au traitement des données sont fixées par la loi sur la fonction de police[3] complétées par la loi du 30 juillet 2018 sur la protection des données[4] qui assure la transposition de la directive 2016/680 dite directive « police-justice »[5]. Le contrôle du respect de ces dispositions est assuré par une autorité indépendante, à savoir, l'Organe de contrôle de l'information policière (ci-après C.O.C.). Nous verrons de surcroit que, pour pouvoir exercer ses droits, la personne concernée doit s'élancer dans un véritable « parcours du combattant ». En effet, même si elle peut exercer ses droits auprès du C.O.C. considérant qu'il peut s'avérer impossible pour la personne « fichée » de déterminer quel est le responsable du traitement de ses données, elle n'a toutefois aucun droit d'accès au contenu des informations emmagasinées, le C.O.C. se limitant à répondre qu'il a « procédé aux vérifications nécessaires » sans donner d'informations complémentaires. Ceci exclut, par conséquent, toute possibilité de débat contradictoire dans l'hypothèse où les services de police y encodent des informations inexactes ou parcellaires et prive *a fortiori* la personne concernée du droit à la rectification voire à l'effacement de ses données.

Cadre général

Les banques de données policières et judiciaires opérationnelles

§3 Il existe actuellement en Belgique quatre types de banques de données policières et judiciaires opérationnelles : la B.N.G., les banques de données de base, les banques de données particulières et les banques de données communes. Examinons chacune de celles-ci.

La banque nationale générale

§4 La B.N.G. est la banque de données la plus importante, elle contient les données traitées à des fins de police administrative et judiciaire et les informations dont l'ensemble des services de police ont besoin pour exercer leurs missions. Cette banque de données doit permettre, par exemple, d'identifier des personnes et de vérifier leurs antécédents de police administrative et de police judiciaire mais aussi, de manière plus large, d'assurer la coordination et le croisement des données à caractère personnel et des informations policières[6]. Historiquement, c'est en 1998, suite à l'affaire Dutroux − et des nombreuses critiques qui s'ensuivirent sur les échanges d'informations défaillants −, que la B.N.G. fut créée dans le but d'améliorer la circulation de l'information policière entre les différents services de police[7]. Depuis lors, elle rassemble une masse considérable d'informations utiles à des fins judiciaires ou à des fins administratives, telles les informations communiquées par un indicateur concernant les planifications d'un vol à main armée, l'annonce de l'organisation d'une manifestation à Bruxelles pendant un sommet européen, des informations selon lesquelles des hooligans veulent perturber un match de football en agressant leurs adversaires[8]. Le type d'informations encodées est très varié, le critère étant « l'intérêt concret que cette information présente pour l'exécution des missions de police […] »[9]. S'il s'agit d'informations « douces » c'est-à-dire des données relatives à des faits non-concrets, ces données sont encodées sous la forme de comptes-rendus ou de rapports administratifs (RIR) ou encore, sous la forme de rapports judiciaires[10] (RAR). S'il s'agit d'informations « dures » concernant des faits concrets telle l'audition d'une victime ou d'un témoin, ces données sont encodées sous la forme procès-verbaux (ci-après P.V.)[11]. C'est, en premier lieu, au fonctionnaire de police qui introduit les données dans cette banque de données de s'assurer de la pertinence de celles-ci et d'évaluer si elles sont proportionnelles au but poursuivi[12]. D'après les chiffres disponibles − extrêmement opaques, puisque non publiés officiellement *in extenso* depuis 2008[13] − le succès de cette banque de données est tel qu'une personne sur cinq en Belgique y serait inscrite[14]. En 2017, 2,2 millions de personnes y figureraient. Ce chiffre serait passé à trois millions en 2019[15].

Les banques de données de base et les banques de données particulières

§5 En 2014, le législateur a profondément revu les règles relatives à la gestion de l'information[16], fixant désormais un cadre légal pour les banques de données de base et les banques de données particulières.

Les banques de données de base sont les banques de données policières locales créées au profit de l'ensemble de la police intégrée[17]. Elles ont pour finalité de permettre l'exécution des missions de police administrative et de police judiciaire grâce à l'exploitation des données à caractère personnel et des informations qui y sont incluses et en informant les autorités compétentes de l'exercice de ces missions[18]. En principe elles ne sont accessibles qu'aux membres des services de police à l'origine des données et informations[19].

Parallèlement aux banques de données de base, les chefs de corps, le commissaire général, les directeurs généraux et/ou les directeurs peuvent « dans des circonstances spécifiques » pour « des besoins particuliers » créer des banques de données particulières[20]. Ces banques de données peuvent être mises en place dans le cas où il s'avère techniquement impossible d'alimenter la B.N.G.[21]. Ainsi, une banque de donnée particulière a été créée pour énumérer les œuvres perdues ou volées et pouvoir y intégrer des photographies de celles-ci[22]. De même, la zone de police Bruxelles-Capitale-Ixelles dispose d'une « tagothèque » visant à répertorier et identifier les auteurs de graffitis ou tags apposés sur le territoire de la zone[23]. Ces banques de données peuvent également être mises en place pour des raisons fonctionnelles, si celles-ci ne sont pas intégrées dans la B.N.G., telles les banques de données relatives aux phénomènes de police administrative[24]. Ces banques de données particulières sont extrêmement nombreuses : il en existerait plus de huit cent[25].

Les banques de données communes

§6 Suite aux attentats en Belgique et en France de 2014 et 2015 et dans la foulée des recommandations du « Plan d'action Radicalisme » approuvé par le Conseil National de Sécurité le 14 décembre 2015, le législateur a mis en place les banques de données communes afin de faciliter l'enregistrement et les échanges d'informations liées à la radicalisation et au terrorisme[26]. Elles sont créées par les ministres de l'intérieur et de la justice pour l'exercice conjoint de leurs missions en matière de terrorisme et d'extrémisme pouvant mener au terrorisme à des fins spécifiques déterminées par la loi telles des nécessités stratégiques, tactiques ou opérationnelles[27]. On peut citer, à cet égard, les banques de données concernant les « Foreign Terrorist Fighters » [28] ou encore les « Propagandistes de haine »[29]. La mise en place de ce type de banques de données suppose une déclaration

préalable auprès du Comité R et du C.O.C., ces derniers devant par la suite émettre un avis dans les trente jours de la réception de la déclaration[30]. Il appartient alors au conseil des ministres de déterminer, par arrêté royal, les types de données à caractère personnel traitées, les modalités des traitements (consultation de la banque de données, utilisation des informations, conservation, effacement et sécurité) et les règles de responsabilités en matière de protection des données à caractère personnel[31]. Pour chaque banque de données, « un gestionnaire » et un « responsable opérationnel » doivent être désignés par le Roi[32].

Les règles générales relatives au traitement

§7 Quelque soit la banque de données visée, les services de police peuvent « traiter »[33] certaines informations pour autant qu'elles présentent un caractère « adéquat, pertinent et non excessif » au regard des finalités pour lesquelles elles sont obtenues et pour lesquelles elles sont traitées ultérieurement[34]. Pour le surplus, il appartient aux ministres de l'Intérieur et de la Justice, chacun dans le cadre de leurs compétences et sans préjudice des compétences propres des autorités judiciaires, de déterminer par directives contraignantes les mesures nécessaires en vue d'assurer la gestion et la sécurité des données traitées dans les banques de données de base, particulières ou la B.N.G.[35]. Le ministre de l'Intérieur est en effet le responsable du traitement[36] pour ce qui concerne les données traitées dans le cadre de la police administrative[37] et le ministre de la Justice l'est pour les données traitées dans le cadre de la police judiciaire[38].

§8 Ces deux ministres sont responsables conjointement lorsqu'il s'agit de données traitées dans le cadre de ces deux finalités et pour les banques de données communes. Pour les banques de données particulières, les responsables du traitement sont les chefs de corps, le commissaire général, les directeurs généraux ou les directeurs qui ont décidé de traiter des données collectées et ont déterminé les finalités et les moyens à cet effet[39]. Sont également déterminées par directives générales et contraignantes des ministres de l'Intérieur et de la Justice, les règles d'accès des membres des services de police à la B.N.G. et aux banques de données particulières[40], les modalités de communications des informations traitées par les services de police et l'interrogation de la B.N.G.[41] mais aussi, les modalités relatives à l'interconnexion des banques de données opérationnelles ainsi que celles auxquelles les services de police ont accès par ou en vertu de la loi ou de traités internationaux liant la Belgique[42].

§9 La loi impose par ailleurs de prévoir des « fichiers de journalisation » permettant d'établir notamment le motif de la consultation des données, tel une enquête particulière, ainsi que l'identification de la personne qui a traité ces données[43]. Ces journaux doivent être mis à la disposition du C.O.C. sur demande[44], afin qu'il puisse vérifier la licéité de certains traitements et effectuer des contrôles, en ce compris dans le cadre de procédures disciplinaires internes des autorités compétentes[45]. La durée de conservation des fichiers de journalisation diffère selon chaque banque de données[46]. L'implémentation des logs est un outil crucial en protection des données puisqu'il permet de contrôler les opérations effectuées, de retracer l'activité des utilisateurs et de détecter les utilisations abusives recouvrant dès lors, à la fois, un aspect dissuasif et un aspect sanctionnateur[47]. Toutefois, en dépit de ces garanties qui existaient déjà sous l'empire de l'ancienne législation[48], un rapport du Comité P met en évidence l'importance des consultations illégitimes de banques de données mises à la

disposition des services de police et ceci, en particulier, en dehors du cadre professionnel, généralement pour des motifs d'ordre privés comme la curiosité[49].

Les catégories particulières de données

§10 Les données révélant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, ou l'appartenance syndicale, ainsi que les données génétiques, les données biométriques aux fins d'identifier une personne physique de manière unique[50], celles concernant la santé, la vie sexuelle ou l'orientation sexuelle d'une personne physique sont qualifiées de données « sensibles »[51]. Compte tenu des risques pour les droits et libertés des personnes physiques et du danger de créer des situations discriminatoires, le traitement de ces données[52] n'est autorisé qu'en cas de « nécessité absolue »[53] et pour autant que ce traitement soit assorti de garanties appropriées et qu'il soit autorisé par une loi, le décret, l'ordonnance, le droit de l'Union européenne ou un accord international[54]. À titre illustratif, un accord de coopération[55] permet l'intégration des données issues du 'Passenger Locator Form'[56] (P.L.F.) dans la B.N.G. en vue de veiller au respect de l'application de la quarantaine obligatoire et du test de dépistage obligatoire des personnes pénétrant sur le territoire belge. En dépit des critiques du C.O.C. quant à l'inscription automatique de ces données dans la banque de données policière[57], celles-ci sont systématiquement encodées mais dans une application de la B.N.G. dite « CROSS/BNG »[58] avant d'être effacées après une période de sept jours si aucune infraction n'est constatée[59]. Dans le cas contraire, par exemple parce que le code pour effectuer un test Covid-19 n'a pas été activé, les données P.L.F. font l'objet d'une inscription dans la B.N.G. en raison de la suspicion de la commission d'une infraction pénale[60].

§11 Depuis l'adoption de la loi du 22 mai 2019[61], dans le cadre des missions de police administrative, judiciaire ainsi qu'en matière de coopération policière internationale, les services de police peuvent traiter certaines catégories particulières de données telles que les données de santé, les données biométriques et les données génétiques[62]. Les données biométriques sont, par exemple, les empreintes digitales, les traits du visage, la voix, l'empreinte des oreilles[63]. Elles proviennent notamment de l'enregistrement des caractéristiques des personnes suspectées, du relevé de traces sur les scènes de crime, voire de l'échange international de données[64]. La collecte de ces données est particulièrement sensible en raison de la possibilité qu'elles offrent de tirer des conclusions quant à l'origine ethnique et à la santé[65]. Elles ne peuvent être traitées qu'à des fins d'identification des personnes en complément de celles déjà visées par la loi sur la fonction de police et sous réserve du respect de certaines conditions lesquelles diffèrent selon le statut de la personne concernée, qu'elle soit victime ou suspecte, par exemple[66].

§12 Concernant les données de santé, elles ne peuvent être traitées que pour « comprendre le contexte lié à la personne concernée ainsi que pour assurer la sécurité et protéger la santé de toute personne susceptible d'entrer en contact

avec les personnes concernées dans le cadre de l'intervention policière »[67]. Les travaux préparatoires indiquent en effet que lors d'une intervention des services de police, les intervenants – avocat, traducteur, personnel de secours, fonctionnaire de police – « courent toujours le risque d'être contaminés par des maladies hautement contagieuses » pouvant nécessiter un traitement rapide[68]. Ils précisent également qu'il peut s'avérer utile de connaitre, en fonction d'informations obtenues lors de précédentes interpellations, les raisons d'un changement d'humeur soudain ou d'anticiper une réaction de panique dans le cas où la personne doit être enfermée[69]. Bien que la loi impose de mentionner si les données proviennent ou non d'un professionnel de soins de santé[70], on peut s'inquiéter de la durée de conservation de ces données sans réexamen périodique alors que la santé d'une personne n'est pas figée mais évolue et que l'inexactitude de ces données entraîne un risque de discriminations. Ainsi, en 2003, le Comité P avait déjà constaté dans plusieurs dossiers que ce type d'informations était utilisé sans les précautions suffisantes[71]. Dans un cas précis, il s'agissait d'une personne qui aurait été porteuse du virus du sida et aurait eu l'intention de contaminer les fonctionnaires de police lors d'une intervention policière. Il est ressorti de l'enquête menée par le Comité P et par le C.O.C. que l'information enregistrée relative au virus reposait uniquement sur des rumeurs verbales, qu'il n'y avait aucune justification judiciaire ou administrative de procéder à cet enregistrement, que l'information reçue n'avait pas été évaluée de manière approfondie et qu'il n'y avait pas d'intérêt concret à la conserver dans la banque de données[72].

Les catégories de personnes concernées

§13 L'article 44/5 de la loi sur la fonction de police définit les différentes catégories de personnes dont les données à caractère personnel peuvent être traitées dans la B.N.G., les banques de données de base ou les banques de données particulières[73] aux fins, d'une part, de police administrative[74] et, d'autre part, de police judiciaire[75]. À des fins administratives, il s'agit notamment des données de contact des représentants des associations[76], des personnes impliquées dans des phénomènes de police administrative[77], des membres d'un groupement national ou international susceptible de porter atteinte à l'ordre public[78], des personnes susceptibles de porter atteinte aux personnes ou aux biens mobiliers et immobiliers à protéger[79], des personnes enregistrées en police judiciaire pour un fait infractionnel commis dans le cadre du maintien de l'ordre public[80], des personnes faisant l'objet d'une mesure administrative prise par une autorité administrative compétente et que les services de police sont chargés de suivre par ou en vertu de la loi, du décret ou de l'ordonnance[81].

À des fins judiciaires, il s'agit notamment des données relatives aux suspects d'un fait pénal et aux personnes condamnées[82], des auteurs et suspects d'une infraction sanctionnée administrativement et constatée par la police[83], des personnes décédées de manière suspecte[84], des personnes disparues[85], des personnes évadées ou qui ont tenté de s'évader[86], des données relatives à l'exécution des peines et à leurs modalités d'exécution (par exemple, la libération conditionnelle[87])[88], des témoins d'un fait pénal[89], des infiltrants civils, des indicateurs et des témoins menacés[90], des victimes d'un fait pénal[91] ainsi que les données relatives aux personnes qui se sont constituées partie civiles ou personnes lésées[92] et les personnes civilement responsables d'un fait pénal[93]. Pour le traitement des données des mineurs de moins de quatorze ans accomplis, l'autorisation du magistrat compétent est requise[94], les mineurs de quatorze ans ou plus sont soumis au régime ordinaire, le législateur considérant qu'ils peuvent faire l'objet de sanctions administratives eu égard à la loi du 24 juin 2013 relative aux sanctions administratives communales mais aussi à la loi du 21 décembre 1998 relative à la sécurité lors des matches de football[95].

La durée de conservation des données

§14 La durée de conservation des données diffère en fonction du type de banques de données, de la catégorie de personne concernée, de la gravité des faits en cause et de la finalité pour lesquelles ces données sont enregistrées à savoir, à des fins de police administrative ou judiciaire.

Pour la B.N.G. par exemple, les données des représentants d'associations traitées à des fins de police administrative, communiquées volontairement par celles-ci ou disponibles publiquement pour permettre la gestion des événements, sont conservées pendant trois ans tandis que les données relatives aux personnes impliquées dans les « phénomènes de police administrative » tels le squattage ou les nuisances autour des gares[96] sont conservées pendant cinq ans[97]. En revanche, les données traitées dans la B.N.G. à des fins de police judiciaire sont conservées durant un an, dix ans ou trente ans selon qu'il s'agit d'une contravention, d'un délit ou d'un crime, que la personne soit, par exemple, victime, suspecte ou condamnée[98]. Pour les banques de données de base, la loi prévoit qu'en principe, les données relatives aux missions de police administrative sont accessibles durant cinq ans tandis que celles traitées à des fins judiciaires sont accessibles durant quinze ans à dater de leur enregistrement[99], sous réserve de prolongations[100]. Si les données ont été traitées dans le cadre d'une information ou d'une instruction judiciaire, les données sont accessibles durant trente ans, voire quarante ans, à partir du moment où la fin de l'enquête a été communiquée par le magistrat compétent à la police[101]. Les données traitées dans les banques de données particulières ne sont soumises à aucun délai spécifique considérant que les données doivent être supprimées dès que les besoins particuliers pour lesquels les banques de données ont été érigées disparaissent[102]. Pour les banques de données communes, les données sont conservées en principe maximum trente ans après le dernier traitement[103]. Il est toutefois examiné au minimum tous les trois ans si les données présentent toujours un lien direct avec la finalité pour laquelle la banque de données fut mise en place[104].

§15 Une fois, la durée de conservation des données écoulée, ces données doivent être archivées et donc rendues inaccessibles[105], puis, enfin être effacées à l'issue du délai fixé par la loi[106]. Pour la B.N.G. par exemple, les données sont archivées pendant trente ans puis effacées[107]. Soulignons cependant qu'en théorie, indépendamment de ces périodes de conservation, les données traitées dans les banques de données policières et judiciaires devraient être archivées lorsqu'elles sont devenues non adéquates, non pertinentes ou excessives[108]. En effet, il existe, dans le chef de l'inspecteur de police ayant encodé les données, une obligation d'effacer des banques de données les données qui ne remplissent plus ces critères[109]. *A contrario,* la rétention d'informations, soit le fait de ne pas encoder d'informations susceptibles de présenter un intérêt pour l'exécution de missions de

police, peut faire l'objet de sanctions pénales à l'égard de l'inspecteur de police concerné[110].

En pratique, toutefois, on voit que cela n'a rien d'automatique, certaines informations restant encodées indépendamment de leur validité[111]. Du surcroît, la durée de conservation des données est souvent largement dépassée[112]. Ces données sont dès lors susceptibles d'être conservées, sans être archivées voire effacées, sans limite de temps[113]. En ce sens, dans son rapport d'activités de 2020, le C.O.C. souligne qu'environ 75,69 % des dossiers traités en 2020 (109 dossiers sur 144) introduits sur plainte de la personne concernée, se sont soldés par un archivage/effacement complet ou partiel des enregistrements effectués par la police[114]. Selon le C.O.C., « il s'agit ni plus ni moins d'un chiffre alarmant qui prouve ce que le C.O.C. observe aussi dans le cadre de ses activités, à savoir que la qualité (l'exactitude et la précision) des banques de données policières laisse encore (trop) à désirer » [115]. A cet égard, on lira avec intérêt que, dans l'arrêt M.K. c. France, la Cour européenne des droits de l'Homme a condamné l'Etat français alors qu'il prévoyait un délai de conservation de 25 ans10 alors qu'il s'agit d'un délai inférieur à celui prévu par la loi belge et que, comme nous le verrons *infra*, demander l'effacement des données peut s'avérer un exercice périlleux.

Le contrôle par une autorité indépendante

§16 Le C.O.C. est chargé de surveiller l'application des dispositions contenues dans le titre 2 de la loi du 30 juillet 2018[116], de veiller à la légalité du contenu de la B.N.G., des banques de données de base, des banques de données particulières et des banques de données techniques, ainsi que de la procédure de traitement des données et informations qui y sont conservées[117]. Il peut également émettre des avis, d'initiative ou sur demande, sur toute question relative à la gestion de l'information policière[118].

En outre, le C.O.C. est l'instance compétente pour assurer le suivi des réclamations et des plaintes[119]. Il est tenu d'informer l'auteur de la réclamation de l'état d'avancement et de l'issue de l'enquête dans un délai raisonnable, notamment si un complément d'enquête ou une coordination avec une autre autorité de contrôle est nécessaire[120]. Il a le pouvoir de rappeler à l'ordre les différentes autorités compétentes soumises à son contrôle en cas de violation d'une disposition de la règlementation relative aux traitements des données à caractère personnel[121] mais aussi d'ordonner de mettre un traitement en conformité avec la réglementation applicable[122], ou encore d'interdire temporairement ou définitivement un traitement de données[123]. Ainsi, en 2019, le C.O.C. a adopté une mesure correctrice visant à mettre un terme à la surveillance par caméras avec reconnaissance faciale exercée en toute illégalité par la police fédérale à l'aéroport de Zaventem[124].

Pour mener à bien ses missions, il dispose d'un service d'enquête pouvant procéder à l'audition de personnes[125], accéder de manière illimitée aux informations et aux données traitées par les services soumis à son contrôle mais aussi aux locaux où se trouvent ces données[126]. Au besoin, ce service peut requérir l'assistance de la force publique et effectuer les constations qui s'imposent[127] mais aussi, saisir dans ces lieux tous les objets, documents et données d'un système informatique utiles pour son enquête, à l'exception de ceux qui concernent une information ou une instruction judiciaire en cours[128]. Notons que tous les services de l'Etat, y compris les parquets et les greffes des cours et tribunaux sont tenus, vis-à-vis du C.O.C., de ses membres ou des membres du service d'enquête, de fournir à leur demande tous les renseignements qu'ils estiment utiles au contrôle du respect de la législation dont ils sont chargés, ainsi que de leur produire tous les supports d'information voire des copies sous n'importe quelle forme[129]. Toutefois, si ces renseignements font partie d'une enquête pénale ou judiciaire en cours, ils ne seront transmis que moyennant l'autorisation préalable du magistrat compétent[130].

Les droits des personnes concernées

§17 Les droits des personnes concernées, à savoir, le droit à l'information, le droit d'accès, le droit à la rectification ou l'effacement, ne sont pas encadrés par la loi sur la fonction de police mais de manière générique, par la loi du 30 juillet 2018[131]. Comme nous l'examinerons dans le cadre de cette section, cette carence pose certaines difficultés qui, par voie de conséquence, porte atteinte à l'effectivité des droits des personnes concernées.

Nous verrons également que, de manière spécifique, lorsque les données à caractère personnel figurent dans une décision judiciaire ou un dossier judiciaire, ou font l'objet d'un traitement lors d'une enquête judiciaire et d'une procédure pénale, toute demande d'accès, de rectification ou d'effacement doit être adressée au ministère public ou au juge d'instruction conformément aux modalités fixées par le Code d'instruction criminelle, le Code judiciaire ou les lois particulières[132].

Le droit à l'information

§18 En principe, afin de garantir l'effectivité de ses droits, la personne concernée doit pouvoir obtenir du responsable du traitement des informations relatives au traitement, de manière accessible, en termes clairs, simples et faciles à comprendre et ce, par tout moyen approprié, y compris par voie électronique[133]. Plus précisément, le responsable du traitement est tenu de fournir à la personne concernée les informations suivantes : l'identité du responsable du traitement, le cas échéant, les coordonnées du délégué à la protection des données ; l'existence d'un traitement ; les finalités du traitement ; le droit d'introduire une plainte auprès de l'autorité de contrôle et les coordonnées de ladite autorité ; l'existence du droit d'accès, de rectification, d'effacement, de la limitation du traitement ; la base juridique du traitement ; la durée de conservation des données à caractère personnel ou, lorsque cela n'est pas possible, les critères utilisés pour déterminer cette durée ; et, le cas échéant, les catégories de destinataires des données à caractère personnel[134].

Pour assurer un traitement loyal des données, des informations complémentaires peuvent être fournies à la personne concernée en particulier, lorsque ses données sont collectées à son insu, par des moyens secrets ou non[135]. Selon le législateur, ces informations peuvent figurer sur le site Internet de l'autorité compétente de sorte qu'il ne s'agirait pas d'une obligation de notification individuelle[136]. On peut toutefois se demander si cette approche est conforme à l'esprit de la directive 2016/680 dans la mesure où ces informations complémentaires visent justement à permettre à la personne concernée de faciliter l'exercice de ses droits[137]. Ainsi, dans le cadre d'un avis relatif à la loi sur les sanctions administratives communales, la Commission de la protection de la vie privée recommandait de fournir des informations complémentaires à la personne concernée « dès l'enregistrement des données » lorsque les informations n'étaient pas collectées auprès de celle-ci mais par d'autres moyens tels que la plaque d'immatriculation d'une voiture[138].

§19 S'agissant du domaine pénal, le législateur peut cependant prévoir qu'aucune information ne pourra être communiquée à la personne concernée lorsqu'une telle mesure est nécessaire et proportionnée par rapport à l'objectif poursuivi, tel que « les nécessités de l'enquête »[139]. Ni la directive 2016/680 ni la loi du 30 juillet 2018 n'indiquent toutefois clairement si cette dernière doit être informée du traitement réalisé dès lors que le refus de fournir ces informations ne se justifie plus par exemple, en raison de la clôture de l'enquête. La CJUE souligne l'importance de cette exigence dans son avis 1/2015, celle-ci estimant qu'« il importe que les passagers aériens soient informés du transfert de leurs données PNR vers le Canada et de l'utilisation de ces données dès le moment où cette communication n'est pas susceptible de compromettre les enquêtes conduites par

les autorités publiques » considérant qu'« une telle information s'avère, de fait, nécessaire pour permettre aux passagers aériens d'exercer leurs droits de demander l'accès aux données PNR les concernant et, le cas échéant, la rectification de celles-ci ainsi que d'introduire, conformément à l'article 47, premier alinéa, de la Charte [des droits fondamentaux de l'Union européenne], un recours effectif devant un tribunal »[140]. En ce sens également, dans le cadre de l'affaire *Schrems II*, l'avocat général près la CJUE rappelle qu'« il ressort de la jurisprudence que les autorités d'un État membre sont, en principe, tenues de notifier l'accès aux données dès le moment où la notification n'est plus susceptible de compromettre les enquêtes menées. Une telle notification constitue, en effet, un prérequis à l'exercice du droit de recours au titre de l'article 47 de la Charte. Cette obligation est désormais reprise à l'article 23, paragraphe 2, sous h), du RGPD »[141]. S'agissant d'un droit fondamental, on peut donc regretter que cette obligation de notification individuelle « *a posteriori* » ne soit pas expressément ancrée dans la loi du 30 juillet 2018 afin de faciliter l'exercice de leurs droits.

Le droit d’accès

§20 L’article 38, §1 de la loi du 30 juillet 2018, s’alignant sur la directive 2016/680, consacre le droit d’accès direct, c’est-à-dire auprès du responsable du traitement, en tant que règle générale et ce, conformément à l’article 8, §2 de la Charte[142]. Sur demande de la personne concernée, le responsable du traitement doit donc mettre à la disposition de celle-ci dans les meilleurs délais et en tout état de cause dans un délai d’un mois[143], la copie des données la concernant mais aussi certaines informations telles que : la confirmation que des données à caractère personnel la concernant sont ou ne sont pas traitées ; les données à caractère personnel en cours de traitement et toute information disponible quant à leur source[144]. Elle doit également informer la personne concernée de la possibilité d’en demander la rectification, l’effacement voire la limitation du traitement eu cause et au besoin, de la possibilité d’introduire une plainte auprès de l’autorité de contrôle[145].

§21 Conformément à l’article 42, al. 1 de la loi du 30 juillet 2018, vu la difficulté pour la personne concernée d’identifier le responsable du traitement[146], la personne concernée peut exercer son droit d’accès par l’intermédiaire du C.O.C. sans préjudice de l’exercice de ses droits auprès du responsable du traitement. En ce cas, le C.O.C. se limite à indiquer qu’il a été procédé aux vérifications nécessaires sans communiquer d’informations contextuelles voire sans indiquer si des données traitées par les services de police, ont été rectifiées ou supprimées[147]. Le C.O.C. justifie cette limitation sur la base de l’article 42, al. 3 et 4 de la loi du 30 juillet 2018 selon lequel certaines informations contextuelles peuvent être communiquées aux personnes concernées selon les modalités fixées par arrêté royal lequel fait toujours actuellement défaut[148]. Cette pratique n’est toutefois pas conforme à l’article 38, §2 de cette même loi selon lequel c’est à la loi, le décret ou l’ordonnance de limiter entièrement ou partiellement le droit d’accès de la personne concernée, dès lors et aussi longtemps qu’une telle limitation partielle ou totale constitue une mesure nécessaire et proportionnée dans une société démocratique, en tenant dûment compte des droits fondamentaux et des intérêts légitimes de la personne physique concernée en fonction de l’objectif poursuivi[149]. Or, aucune disposition légale spécifique ne limite explicitement le droit d’accès[150]. À l’inverse, considérer que l’article 42, al. 1 de la loi du 30 juillet 2018 limite totalement le droit d’accès à l’égard des services de police[151] reviendrait à admettre qu’un seul article de cette loi puisse limiter l’exercice des droits des personnes concernées pour l’ensemble des bases de données policières, et sans tenir compte des critères susmentionnés.

§22 Un tel raisonnement aboutirait donc à généraliser un système d’exception à un droit fondamental, ce qui entre en contradiction avec l’esprit de la directive 2016/680[152]. Selon nous, l’instauration d’une limitation du droit d’accès à l’égard des banques de données policières suppose nécessairement que celle-ci soit

encadrée dans chaque base légale spécifique les régissant dans le respect des critères de nécessité et proportionnalité[153]. En effet, l'accès aux données revêt une importance fondamentale puisqu'il constitue un prérequis pour l'exercice d'autres droits comme le droit à la rectification et le droit à l'effacement[154]. En ce sens, à l'occasion de l'arrêt *Schrems II,* l'avocat général près la CJUE indique : « le droit d'accès implique la possibilité pour une personne d'obtenir des autorités publiques, sous réserve des dérogations strictement nécessaires à la poursuite d'un intérêt légitime, la confirmation du fait qu'elles traitent ou non des données à caractère personnel la concernant »[155]. Or, en se limitant à indiquer à la personne concernée que les vérifications nécessaires ont été faites, cette dernière est privée du droit de savoir si des informations la concernant sont traitées par les autorités policières et dès lors, d'en demander la rectification ou l'effacement.

§23 Précisons cependant que, concernant spécifiquement les données traitées dans le cadre d'une enquête pénale, lors d'une information ou d'une instruction, le droit d'accès s'exerce auprès du procureur du Roi ou du juge d'instruction conformément aux modalités fixées par le Code d'instruction criminelle[156]. En ce cas, la personne concernée dispose d'un droit d'accès au dossier répressif qui peut être limité pour certains besoins particuliers tels que les « nécessités de l'enquête »[157].

Le droit à la rectification et l'effacement

§24 La personne concernée a également le droit d'obtenir du responsable du traitement, dans les meilleurs délais, la rectification ou la complétion voire l'effacement des données à caractère personnel la concernant lorsque celles-ci sont inexactes[158]. Le responsable du traitement peut, au lieu de procéder à l'effacement, limiter le traitement si l'exactitude des données à caractère personnel est contestée par la personne concernée et qu'il ne peut être déterminé si les données sont exactes ou non, ou si les données à caractère personnel doivent être conservées à des fins probatoires[159]. Le responsable du traitement informe par la suite la personne concernée par écrit des rectifications effectuées ou, de manière motivée, du refus éventuel de rectifier ou d'effacer ses données[160].

§25 Comme exposé *supra* pour l'exercice du droit d'accès, lorsque la personne concernée exerce ses droits par l'intermédiaire de l'autorité de contrôle, à savoir, le C.O.C., celui-ci se limite à indiquer systématiquement qu'il a procédé aux vérifications nécessaires[161]. Il peut donc s'avérer impossible pour la personne concernée de savoir si des données ont été rectifiées ou effacées. Outre le fait que cet approche n'est pas conforme à l'esprit de la directive 2016/680, ceci est interpellant d'autant que dans l'arrêt *M.K. c. France* du 18 avril 2013, la Cour européenne des droits de l'Homme a condamné l'Etat français entre autres en raison du fait que « l'effacement, qui n'est au demeurant pas un droit, constitue une garantie ''théorique et illusoire'' et non ''concrète et effective'' »[162].

§26 Précisons par ailleurs que, pour les catégories d'informations extraites de décisions judiciaires coulées en force de chose jugée susceptibles d'avoir une incidence sur les données traitées dans la B.N.G. telles qu'une décision d'acquittement, un changement de qualification des faits, une ordonnance de non-lieu, la personne concernée peut introduire une requête auprès du procureur du Roi pour demander que ces informations soient transmises auprès des autorités compétentes[163]. Il en est de même pour les catégories d'informations extraites de décisions de classement sans suite pour charges insuffisantes ou pour absence d'infraction, prises par le ministère public[164]. En effet, en principe, ces informations sont communiquées endéans les trente jours aux services de police selon les modalités fixées par arrêté royal[165]. Toutefois, aucun arrêté royal n'ayant été adopté, la transmission d'informations ne semble toujours pas revêtir un caractère systématique[166]. Les informations obsolètes sont donc susceptibles de rester encodées dans les banques de données sans limite de temps en l'absence de proactivité de la personne concernée.

Conclusion

§27 Après l'adoption du titre 2 de la loi du 30 juillet 2018 fixant le cadre général relatif au traitement de données par les services de police, le législateur a complété la loi sur la fonction de police quant aux règles relatives aux traitements de données à caractère personnel par les services de police[167]. Même si ces modifications devaient renforcer les garanties applicables en la matière, en pratique, le respect de ces règles n'est pas exempt de critiques. Dans son rapport annuel de 2020, le C.O.C. constate par exemple que « la BNG contient de nombreuses inexactitudes et/ou erreurs, alors qu'il s'agit de la banque de données qui contient des données validées, et notamment : – des délais de conservation (largement) dépassés ; – une qualification erronée conférée aux faits ; – des motifs d'enregistrement erronés ou caducs ; – des rapports d'information dont le délai de conservation est dépassé ou qui n'ont plus aucune pertinence ; – des signalements qui restent ouverts sans aucune valeur ajoutée ni évaluation intermédiaire ; – etc. »[168].

Outre les conséquences préjudiciables qu'un tel fichage peut avoir pour la personne concernée, celle-ci peine à pouvoir exercer ses droits. Comme nous l'avons vu, elle n'est pas en mesure d'être informée si des données la concernant sont traitées par les services de police (ou ont été traitées), ne disposant d'aucun droit à l'information individuelle et ce, même, *a posteriori,* lorsque l'objectif poursuivi par la limitation ne se justifie plus. De surcroît, elle ne peut accéder aux données qui la concerne, le C.O.C. se limitant à indiquer qu'il a procédé aux vérifications nécessaires sans communiquer d'autres informations contextuelles. Par voie de conséquences, elle est également privée de la possibilité de demander la rectification ou l'effacement de ses données et donc, de l'exercice d'un recours effectif au sens de l'article 47 de la Charte. Or, cette limitation systématique de l'exercice d'un droit fondamental garanti par l'article 8, §2 de la Charte des droits fondamentaux entre en contradiction avec le respect des critères de nécessité et de proportionnalité exigés en cas d'ingérence dans ce droit. Enfin, elle prive la personne condamnée voire de manière plus large, la personne « connue » des services de police, de toute possibilité de faire corriger des données susceptibles de porter atteinte à ses projets visant à favoriser sa réinsertion dans la société, réinsertion d'autant plus difficile si elle sort de prison.

---

1. Voyez à cet égard les contributions de Christine Guillain et de Vanessa de Greef et Antoine Chomé dans ce dossier. ↩

2. Nous limiterons notre contribution à l'examen des banques de données policières et judiciaires « opérationnelles » lesquelles se différencient des banques de données techniques visées à l'article 44/2, §3 de la loi sur la fonction de police qui sont créées suites à l'utilisation de caméras intelligentes de reconnaissance automatique de plaques d'immatriculation ou de systèmes intelligents de reconnaissance automatique de plaques d'immatriculation. De même, nous n'examinerons pas le cadre légal relatif aux données pénitentiaires à savoir la banque de données

« Sidis Suite » dans laquelle sont traitées les données nécessaires à l'exercice adéquat des missions légales de l'administration pénitentiaire tels que l'exécution des peines et mesures privatives de liberté. (A cet égard voy. loi du 5 mai 2019 portant dispositions diverses en matière d'information de la Justice, de modernisation du statut des juges consulaires et relativement à la banque des actes notariés, *M.B*,. 19 juin 2019). ↩

3. Loi du 5 août 1992 sur la fonction de police, *M.B.*, 22 décembre 1992 (ci-après loi sur la fonction de police). ↩

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

5. Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, *J.O. L 119,* 4 mai 2016, pp. 89–131. ↩

6. Art. 44/7, al. 1er, 3° de la loi sur la fonction de police ↩

7. KAISER V., « La Banque de données nationale générale et le droit d'accès indirect du citoyen aux données à caractère personnel qu'elle contient », *R.D.T.I.*, 2010, n° 43, pp. 3–5. ↩

8. A cet égard voy. les exemples donnés dans la directive commune MFO-3 du 14 juin 2002 des ministres de la Justice et de l'Intérieur relative à la gestion de l'information de police judiciaire et de police administrative, *M.B.*, 18 juin 2002, point 2 3, p 3. ↩

9. *Ibidem*. ↩

10. Exposé des motifs du projet de loi modifiant la loi sur la fonction de police, la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *Doc. Parl.,* Ch., 2013–2014, n°53–3105/001, p. 7. ↩

11. Art. 40 de la loi du 5 août 1992 sur la fonction de police. ↩

12. Art. M2, 2.3. de la directive commune MFO-3 du 14 juin 2002 des Ministres de la Justice et de l'Intérieur relative à la gestion de l'information de police judiciaire et de police administrative, *M.B.*, 18 juin 2002 (ci-après Directive commune MFO-3). ↩

13. Les derniers chiffres publiés sont disponibles dans le Rapport annuel du Comité P, 2007, p. 36, disponible sur le site Internet du Comité P (http://www.comitep.be). ↩

14. À cet égard, voy. BAILLY O., « La banque de données non gérée », *Medor*, 14 avril 2021. ↩

15. *Ibidem*. ↩

16. Loi du 18 mars 2014 relative à la gestion de l'information policière et modifiant la loi du 5 août 1992 sur la fonction de police, la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel et le Code d'instruction criminelle, *M.B.,* 28 mars 2014. ↩

17. Art. 44/11/2, §1 de la loi sur la fonction de police. La police locale et la police fédérale constituent ensemble la police intégrée. À cet égard voy. la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux, *M.B.*, 5 janvier 1999. ↩

18. Art. 44/11/2, §1 de la loi sur la fonction de police. ↩

19. *Doc. parl.,* Ch., 2013–2014, DOC 53–3105/001, pp. 7–8 ↩

20. Art. 44/11/3, §2 de la loi sur la fonction de police. ↩

21. Art. 44/11/3, al. 1 de la loi sur la fonction de police. ↩

22. Exposé des motifs du projet de loi modifiant la loi sur la fonction de police, la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *Doc. Parl.,* Ch.., 2013–2014, n°53–3105/001, p. 7. ↩

23. Rapport d'activité 2012 de la zone de police Bruxelles-Capitale - Ixelles. ↩

24. *Doc. parl.,* Ch., 2013–2014, DOC 53–3105/001, pp. 7–8. Il s'agit de l'ensemble des problèmes, portant atteinte à l'ordre public et nécessitant des mesures appropriées de police administrative, parce qu'ils sont de même nature et répétitifs, qu'ils sont commis par les mêmes personnes ou qu'ils visent les mêmes catégories de victimes ou de lieux ↩

25. Dans un avis du 31 mars 2017, le C.O.C en a analysé environ huit cent. Par souci de transparence, on peut regretter que ledit avis n'ait pas été publié, au moins partiellement ; celui-ci étant uniquement référencé dans l'avis n°009/2018 du 12 décembre 2018 concernant l'avant-projet de loi relatif à la gestion de l'information policière et modifiant la loi sur la fonction de police et la loi du 7 décembre 1998 organisant un service de police intégré, structure à deux niveaux, publié dans *Doc. Parl.,* Ch., 2018–2019, n°54–3697/003, p. 37 et suivants. ↩

26. Projet de loi du 21 mars 2016 relatif à des mesures complémentaires en matière de lutte contre le terrorisme, *Doc. Parl.,* Ch., 2015–2016, n°54–1727/001. ↩

27. Art. 44/11/3*bis* de la loi sur la fonction de police. ↩

28. Arrêté royal du 21 juillet 2016 relatif à la banque de données commune Terrorist Fighters. ↩

29. Arrêté royal du 23 avril 2018 modifiant l'Arrêté royal du 21 juillet 2016 relatif à la banque de données commune Foreign Terrorist Fighters portant exécution de certaines dispositions de la section 1er*bis* « de la gestion des informations » du chapitre IV de la loi sur la fonction de police et modifiant la banque de données commune Foreign Terrorist Fighters vers la banque de données commune Terrorist Fighters. ↩

30. art. 44/11/3bis, §3 de la loi sur la fonction de police. ↩

31. art. 44/11/3bis, §4, al.2 de la loi sur la fonction de police. ↩

32. art. 44/11/3bis, §§9 et 10 de la loi sur la fonction de police. ↩

33. On entend par traitement de données à caractère personnel, toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction des données. Voy. art. 26, 2° de la loi du 30 juillet 2018. ↩

34. Art. 44/1, § 1er, de la loi sur la fonction de police. ↩

35. Il s'agit notamment des aspects relatifs à la fiabilité, la confidentialité, la disponibilité, la traçabilité et l'intégrité des données à caractère personnel (art. 44/4, §2, de la loi sur la fonction de police). ↩

36. Selon l'article 26, 8°, de la loi du 30 juillet 2018, le responsable du traitement est défini comme étant « l'autorité compétente qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel ». La loi précise toutefois que « Lorsque les finalités et les moyens de ce traitement sont déterminés par la loi, le décret ou l'ordonnance, le responsable du traitement est l'entité désignée comme responsable du traitement par ou en vertu de cette loi, ce décret ou cette ordonnance ». ↩

37. Art. 44/4, §1er, al. 1er de la loi sur la fonction de police. ↩

38. Art. 44/4, §1er, al. 2 de la loi sur la fonction de police. ↩

39. A cet égard, voy. C.O.C., avis d'initiative n° DD2000026 du 11 février 2021 concernant la question de savoir qui est le responsable du traitement pour les traitements de données par les services de police dans le cadre de l'exécution de missions policières d'une part et pour les traitements de données en vertu du RGPD d'autre part. ↩

40. Art. 44/4, §3, de la loi sur la fonction de police. Voy. à cet égard : Directive commune contraignante des Ministres de la Justice et de l'Intérieur relative aux règles d'accès des membres des services de police à la banque de données nationale générale, aux banques de données de base, particulières et techniques, *M.B.,* 13 juillet 2017. ↩

41. Directive commune des Ministres de la Justice et de l'Intérieur relative à la détermination des modalités de communication des données à caractère personnel et informations traitées dans le cadre de leurs missions de police administrative et judiciaire, telles que visées aux articles 14 et 15 de la loi sur la fonction de police, par les services de police et à l'accès direct et l'interrogation directe de la BNG, *M.B.,* 2 février 2021. ↩

42. Art. 44/4, §4, de la loi sur la fonction de police. Voy. à cet égard : Directive contraignante commune des Ministres de la Justice et de l'Intérieur relative aux modalités relatives à l'interconnexion des banques de données visées à l'article 44/2 entre elles ou avec d'autres banques de données auxquelles les services de police ont accès par ou en vertu de la loi ou de traités internationaux liant la Belgique, *M.B.,* 4 août 2021. Cette directive a par ailleurs fait l'objet de nombreuses critiques du C.O.C. en raison de son imprécision mais aussi en raison de l'absence de limite relative à l'interconnexion entre les différentes banques de données policières lesquelles peuvent de surcroît comprendre des informations non validées. Voy. C.O.C., Avis n° DA200009 du 22 septembre 2020, relatif à une directive commune des ministres de la Justice et de l'Intérieur relative aux modalités relatives à l'interconnexion des banques de données visées à l'article 44/2 entre elles ou avec d'autres banques de données auxquelles les services de police ont accès par ou en vertu de la loi ou de traités internationaux liant la Belgique (directive relative à l'interconnexion). ↩

43. Art. 44/4, §2 de la loi sur la fonction de police. ↩

44. Art. 56, §3 de la loi du 30 juillet 2018. ↩

45. Art. 56, §1, al. 3 de la loi du 30 juillet 2018. ↩

46. Pour la B.N.G. par exemple, l'enregistrement des « logs » relatifs aux accès est prévu pour une période de dix ans minimum. (Art. 44/11/12, §2, e), 2° de la loi sur la fonction de police.) ↩

47. Groupe 29, opinion on some key issues of the Law Enforcement (EU 2016/680), WP258, 29 novembre 2017, p. 26 (ci-après Groupe 29, avis 2017). Le Groupe de Travail de l'Article 29 est un organe consultatif européen indépendant sur la protection des données. Depuis le 25 mai 2018, le Comité Européen de la Protection des données lui a succédé. Dans le cadre de cette contribution nous ferons cependant référence au Groupe 29, les avis ayant été adoptés sous l'empire de la directive 95/46/CE (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, p. 31). ↩

48. A cet égard voy. KAISER V., « La Banque de données nationale générale et le droit d'accès indirect du citoyen aux données à caractère personnel qu'elle contient », *R.D.T.I.*, 2010, n° 43. ↩

49. Comité P, *Rapport établi dans le cadre de l'enquête de contrôle relative aux accès illégitimes aux banques de données par les membres des services de police*, Dossier n°21530/2015. Voy. également le Comité P, *Rapport annuel 2017*, p. 108, disponible sur le site Internet du Comité P (http://www.comitep.be). ↩

50. À ce propos voy. JASSERAND C., « Legal Nature of Biometric Data: From « Generic » Personal Data to Sensitive Data », *E.D.P.L*, 2016/3, pp. 297–311. ↩

51. Art. 34, §1 de la loi du 30 juillet 2018. ↩

52. Art. 10 de la directive 2016/680. ↩

53. Dans l'avis du Groupe 29 précité, il est fait référence à l'expression « strictement nécessaire » et non à la « nécessité absolue » et ce, conformément à la jurisprudence de la CJUE dans le cadre des arrêts récents relatifs à la protection des données (voy. entres autres : CJUE, 6 octobre 2015, *Schrems c. Data Protection Commissionner of Ireland,* C-362/14 ; C.J.U.E., 8 avril 2014, *Digital Rights Ireland Ltd & Michael Seitlinger e.a.*, C-293/12 & C-594/12 ; CJUE, 21 décembre 2016, *Tele2 Sverige AB/Post-och telestyrelsen et Secretary of State for the Home Department/Tom Watson e.a.,* affaires jointes C-203/15 & C-698/15). On peut toutefois raisonnablement considérer que ces termes sont équivalents. Selon le Groupe 29, l'utilisation de ces termes vise à mettre l'accent sur le respect du principe de nécessité en raison du traitement de catégories particulières de données mais aussi sur l'importance de prévoir des justifications solides pour le traitement de telles données (Groupe 29, avis 2017, p. 9). ↩

54. Art. 34, §1, 1° de la loi du 30 juillet 2018. ↩

55. Accord de coopération du 24 mars 2021 entre l'Etat fédéral, la Communauté flamande, la Région wallonne, la Communauté germanophone et la Commission communautaire commune concernant le transfert de données nécessaires aux entités fédérées, aux autorités locales ou aux services de police en vue du respect de l'application de la quarantaine ou du test de dépistage obligatoires des voyageurs en provenance de zones étrangères et soumis à une quarantaine ou à un test de dépistage obligatoires à leur arrivée en Belgique, *M.B.*, 24 mars 2021. ↩

56. Conformément à l'article 21 de l'arrêté ministériel portant des mesures d'urgence pour limiter la propagation du coronavirus COVID-19 du 28 octobre 2020 (*M.B.*, 28 octobre 2020), les personnes en provenance de l'étranger vers la Belgique doivent compléter un formulaire de « localisation du passager ». ↩

57. C.O.C., avis n° DA210007 du 16 mars 2020 relatif au projet d'accord de coopération entre l'État fédéral, la Communauté flamande, la Région wallonne, la Communauté germanophone et la Commission communautaire commune concernant le transfert de données nécessaires aux entités fédérées, aux autorités locales ou aux services de police en vue du respect de l'application de la quarantaine ou du test de dépistage obligatoires des voyageurs en provenance de zones étrangères et soumis à une quarantaine ou à un test de dépistage obligatoires à leur arrivée en Belgique, p. 5. ↩

58. La Police Fédérale a déployé la première version de l'application **BNG/CROSS** le 22 novembre 2019. Dans le cadre de la gestion des infractions dues au Covid-19, une version spécifique (CROSS COVID) a été mise en place. Cette application permet notamment le signalement et la perception immédiate des infractions Covid depuis la première phase de confinement (avril 2020). Voy. le rapport annuel de 2020 de la police fédérale disponible sur : https://rapportannuel.policefederale.be/. ↩

59. Nous nous basons sur les informations dévoilées par Monsieur SCHUERMANS dans un interview publié dans le magazine Medor. Voy. BAILLY O., « Des centaines de milliers de voyageurs bientôt dans la base de données policières », *Medor*, publié le 30 avril 2021, disponible sur https://medor.coop/hypersurveillance-belgique-surveillance-privacy/police-justice-bng/episodes/je-peux-imaginer-un-acces-differencie-bng-65-voyage-fichage-plf-tracing/?full=1#continuer-a-lire ↩

60. *Ibidem*. ↩

61. Loi du 22 mai 2019 modifiant diverses dispositions en ce qui concerne la gestion de l'information policière, *M.B.,* 19 juin 2019. ↩

62. Art. 44/1, §2 de la loi sur la fonction de police. ↩

63. Proposition de loi du 27 mars 2019 modifiant diverses dispositions en ce qui concerne la gestion de l'information policière, *Doc. Parl.,* Ch., 2018–2019, n°54 3697/001, p. 13. ↩

64. *Ibidem*, p. 12. ↩

65. Voy. par exemple : Cour EDH, *S. et Marper c. Royaume-Uni,* 4 décembre 2008, n°30562/04 et n°30566/4 . ↩

66. À titre illustratif, dans le cadre des missions judiciaires, les services de police peuvent traiter les données des suspects d'un fait pénal et des personnes condamnées ou encore des suspects d'une infraction sanctionnée administrativement et constatée par la police (art. 44/5, § 3 1° à 6° de la loi sur la fonction de police). Ils ne peuvent en revanche traiter les données témoins et les victimes d'un fait pénal sans leur consentement à moins que les données ne soient manifestement rendues publiques par la personne concernée ou encore pour sauvegarder les intérêts vitaux de la personne concernée ou d'une autre personne physique (art. 44, § 3, 7° à 9°, et au § 4 de l'article 44/5 de la loi sur la fonction de police). ↩

67. Art. 44, §2, al. 2, 2° de la loi sur la fonction de police. ↩

68. Proposition de loi du 27 mars 2019 modifiant diverses dispositions en ce qui concerne la gestion de l'information policière, *Doc. Parl.,* Ch., 2018–2019, n°54–3697/001, p. 13. ↩

69. Proposition de loi du 27 mars 2019 modifiant diverses dispositions en ce qui concerne la gestion de l'information policière, *Doc. Parl.,* Ch., 2018–2019, n°54–3697/001, p. 14. ↩

70. Art. 44, §2, al. 2, 2° de la loi sur la fonction de police. ↩

71. Comité P, *Rapport annuel 2003*, point. 67, disponible sur : [http://www.comitep.be/2003/Fr/2003FR.htm]. ↩

72. *Ibidem*. ↩

73. Art. 44/11/3, al.2 de la loi sur la fonction de police. ↩

74. Art. 44/5, §1 de la loi sur la fonction de police. ↩

75. Art. 44/5, §3 de la loi sur la fonction de police. ↩

76. Art. 44/5, § 1er, alinéa 1er, 1°, de la loi sur la fonction de police. ↩

77. Art. 44/5, § 1er, alinéa 1er, 2°, de la loi sur la fonction de police. ↩

78. Art. 44/5, § 1er, alinéa 1er, 3°, de la loi sur la fonction de police. La notion de « groupement » n'est pas définie par le législateur. Selon les travaux préparatoires, il s'agit de « un ensemble de personnes avec un certain degré de structuration qui se traduit par exemple par l'organisation de réunions périodiques ou la hiérarchisation, la répartition des rôles entre les membres (rassembler des fonds pour le groupement, recruter pour le groupement, diffuser l'idéologie du groupement, …), ou le port d'un ou plusieurs identifiants communs » (Doc. parl., Ch., 2013–2014, 53–3105/001, p. 28–29.). Une liste est arrêté chaque année par le Ministre de l'Intérieur sur base d'une proposition de la Direction des opérations de police administrative de la police fédérale. A cet égard voy. DETRY I., MINE B. et JEUNIAUX P., « La radicalisation au prisme des banques de données », *Rapport de recherche n° 47, Institut National de Criminalistique et de Criminologie, Direction Opérationnelle de Criminologie,* p. 14. ↩

79. Art. 44/5, § 1er, alinéa 1er, 4°, de la loi sur la fonction de police. ↩

80. Art. 44/5, § 1er, alinéa 1er, 6°, de la loi sur la fonction de police. ↩

81. Art. 44/5, § 1er, alinéa 1er, 7°, de la loi sur la fonction de police. ↩

82. Art. 44/5, § 3, alinéa 1°, de la loi sur la fonction de police. ↩

83. Art. 44/5, § 3, alinéa 2°, de la loi sur la fonction de police. ↩

84. Art. 44/5, § 3, alinéa 3°, de la loi sur la fonction de police. ↩

85. Art. 44/5, § 3, alinéa 4°, de la loi sur la fonction de police. ↩

86. Art. 44/5, § 3, alinéa 5°, de la loi sur la fonction de police. ↩

87. Voyez à cet égard la contribution d'Olivia Nederlandt, Audrey Servais et Audrey Teugels dans ce dossier. ↩

88. Art. 44/5, § 3, alinéa 6°, de la loi sur la fonction de police. ↩

89. Art. 44/5, § 3, alinéa 7°, de la loi sur la fonction de police. ↩

90. Art. 44/5, § 3, alinéa 8°, de la loi sur la fonction de police. ↩

91. Art. 44/5, § 3, alinéa 9°, de la loi sur la fonction de police. ↩

92. Art. 44/5, § 4, alinéa 1°, de la loi sur la fonction de police. ↩

93. Art. 44/5, § 4, alinéa 2°, de la loi sur la fonction de police. ↩

94. Art. 44/7, al. 2 de la loi sur la fonction de police. ↩

95. Sur l'absence de discriminations entre les mineurs de plus de quatorze ans et de moins de quatorze ans voy. C.C., 14 juillet 2016, n°108/2016, B.152.1. ↩

96. DETRY I., MINE B. et JEUNIAUX P, « Description et mise en perspective des données de police administrative relatives aux personnes, groupements et phénomènes à suivre », *Rev. dr. pén.,* 2021/6, p. 618. ↩

97. Art. 44/9, § 1er, al. 1– 2, de la loi sur la fonction de police. ↩

98. Art. 44/9, §2, a), al. 1– 2, de la loi sur la fonction de police. ↩

99. Art. 44/11/2, §2, de la loi sur la fonction de police. ↩

100. Art. 44/11/2, §3, de la loi sur la fonction de police. ↩

101. Art. 44/11/2, §6, de la loi sur la fonction de police. ↩

102. Art. 44/11/3, §4, de la loi sur la fonction de police. ↩

103. Art. 44/11/3bis, §5, al.1 de la loi sur la fonction de police. ↩

104. Art. 44/11/3bis, §5, al.2 de la loi sur la fonction de police. ↩

105. On soulignera que, selon la Cour Constitutionnelle, la durée d'archivage de ces données n'est pas dénué de justification considérant d'une part, qu'après archivage, les données ne peuvent être consultées que dans des situations exceptionnelles, telle que l'enquête sur les tueurs du Brabant wallon, et d'autre part, que le traitement poursuit une autre finalité relevant de la loi relative aux archives (C.C., n°108/2016, 14 juillet 2016, B.113.1.). Certes, durant la période « d'archivage », les données sont légalement consultables à des fins plus limitatives, il reste néanmoins que la personne concernée est en droit de se demander si cette période de rétention n'est pas contraire au prescrit selon lequel les données doivent être conservées « pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées ». ↩

106. Art. 44/1, § 1er, de la loi sur la fonction de police et art. 28, al. 4° de la loi du 30 juillet 2018. ↩

107. Art. 44/10, § 1er, al. 2, de la loi sur la fonction de police. Pour les banques de données de base, voy. art. 44/11/2, §7, de la loi sur la fonction de police. ↩

108. Art. 44/1, § 1er, de la loi sur la fonction de police et art. 28, al. 4° de la loi du 30 juillet 2018. ↩

109. Art. 44/9, § 1er, de la loi sur la fonction de police. ↩

110. Art. 44/11/1, al. 1 de la loi sur la fonction de police. À cet égard voy. Cass. (2e ch.), 22 mai 2018, RG P.17.1286.N, *Pas*., 2018/5, pp. 1109–1113. ↩

111. À cet égard, voy. BAILLY O., « La banque de données non gérée », *Medor*, 14 avril 2021. ↩

112. C.O.C., *Rapport d'activité 2020*, p. 18, disponible sur https://www.organedecontrole.be/files/Rapport-dactivit%C3%A9_COC_2020_F.pdf ↩

113. À cet égard, voy. BAILLY O., *op cit*.. ↩

114. C.O.C., *Rapport d'activité 2020*, *op. cit.* ↩

115. *Ibidem*, p. 17. ↩

116. Art. 71, §1 de la loi du 30 juillet 2018. ↩

117. Art. 239, §1er de la loi du 30 juillet 2018. ↩

118. Art. 236, §1er de la loi du 30 juillet 2018. ↩

119. Art. 240, al.1er, 4° et 247 de la loi du 30 juillet 2018. ↩

120. Art. 240, al.1er, 4° et 247 de la loi du 30 juillet 2018. ↩

121. Art. 247, al.3 de la loi du 30 juillet 2018. ↩

122. Art. 247, al.4 de la loi du 30 juillet 2018. ↩

123. Art. 247, al.5 de la loi du 30 juillet 2018. ↩

124. C.O.C., *Rapport intermédiaire du 16 septembre 2019 avec mesure correctrice concernant la visite menée auprès de la police fédérale de l'aéroport de Zaventem par l'Organe de contrôle de l'information policière et portant sur l'utilisation de la reconnaissance faciale à l'aéroport national de Zaventem*, DIO19005. ↩

125. Art. 245, §1er de la loi du 30 juillet 2018. ↩

126. Art. 244, §1er de la loi du 30 juillet 2018. ↩

127. Art. 244, §3 de la loi du 30 juillet 2018. ↩

128. Art. 244, §2 de la loi du 30 juillet 2018. ↩

129. Art. 246, al.1 de la loi du 30 juillet 2018. ↩

130. Art. 246, al.2 de la loi du 30 juillet 2018. ↩

131. De manière étonnante, lors de l'adoption du titre 2 de la loi du 30 juillet 2018 fixant le cadre général relatif au traitement de données par les services de police, le législateur n'a pas modifié la loi sur la fonction de police en vue d'y intégrer les droits des personnes concernées. ↩

132. Art. 16 de la loi du 30 juillet 2018. ↩

133. Art. 36 et 37 de la loi du 30 juillet 2018. ↩

134. Art. 37, §1, 1° à 8° de la loi du 30 juillet 2018. ↩

135. Art. 37, §1, 9° de la loi du 30 juillet 2018. ↩

136. Projet de loi relatif à la protection des données à caractère personnel, Exposé des motifs, *Doc. Parl.,* Ch., 2017–2018, n° 54–3126/001, p. 80. ↩

137. Considérant 42 de la directive 2016/680. ↩

138. C.P.V.P., avis n°13/2015 du 13 mai 2015 sur l'avant-projet de loi portant dispositions diverses – modifications de la loi portant création d'un organe de recours en matière d'habilitations de sécurité, de la loi sur la fonction de police et de la loi du 18 mars 2014 relative à la gestion de l'information policière (CO-A-2015–019), point 49. ↩

139. Art. 37, §2 de la loi du 30 juillet 2018. On ajoutera qu'en fonction de la sensibilité de certaines bases de données telles celles liées à la lutte contre le terrorisme, le législateur peut prévoir qu'aucune information ne devra être fournie à l'intéressé. Voy. Art. 37, §3 de la loi du 30 juillet 2018. ↩

140. CJUE, Avis 1/2015 du 26 juillet 2017, point 220. ↩

141. *Conclusions de l'Avocat Général. M. Henrik saugmandsgaard øe. présentées* le *19 décembre 2019*, C-311/18, Data Protection Commissioner / Facebook Ireland et Maximillian Schrems, point 320. ↩

142. Selon cette disposition : « Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification ». ↩

143. Art. 38, §1er et 40 de la loi du 30 juillet 2018. ↩

144. Art. 38, §1, 1° à 8° de la loi du 30 juillet 2018. ↩

145. *Ibidem*. ↩

146. Voir ci-avant, les règles générales relatives au traitement. ↩

147. Art. 42, al.2 de la loi du 30 juillet 2018. Cette disposition indique « *« Dans les cas visés aux articles 37, § 2, 38, § 2, 39, § 4, et 62, § 1er, l'autorité de contrôle visée à l'article 71 communique uniquement à la personne concernée qu'il a été procédé aux vérifications nécessaires. »*. ↩

148. Ainsi, l'article 42, al.3 et 4 de la loi du 30 juillet 2018 indique : *« Nonobstant l'alinéa 2, l'autorité de contrôle visée à l'article 71 peut communiquer à la personne concernée certaines informations contextuelles. Le Roi détermine, après avis de l'autorité de contrôle visée à l'article 71, les catégories d'informations contextuelles qui peuvent être communiquées à la personne concernée, par cette autorité de contrôle. »* ↩

149. À savoir : 1° éviter de gêner des enquêtes, des recherches, des procédures pénales ou autres procédures réglementées; 2° éviter de nuire à la prévention ou à la détection d'infractions pénales, aux enquêtes ou aux poursuites en la matière ou à l'exécution de sanctions pénales ; 3° protéger la sécurité publique; 4° protéger la sécurité nationale; 5° protéger les droits et libertés d'autrui. ↩

150. DUMORTIER F. et FORGET C., « Le droit d'accès aux banques de données policières », *J.T.,* 2020, n°6806, pp. 176–178. ↩

151. Art. 41, al. 1 et 42, al. 2 de la loi du 30 juillet 2018. ↩

152. La directive 2016/680, consacre le droit d'accès direct en tant que règle générale et ce, conformément à l'article 8, §2 de la Charte des droits fondamentaux. Voy. Art. 14 de la directive 2016/690. ↩

153. DUMORTIER F. et FORGET C., *op. cit.*,, pp. 176–178. ↩

154. Comité consultatif de la Convention pour la protection des données des personnes à l'égard du traitement automatisé des données à caractère personnel, « Guide pratique sur l'utilisation de données à caractère personnel dans le secteur de la police », Strasbourg, 15 février 2018, p. 7. ↩

155. *Conclusions de l'Avocat Général. M. Henrik saugmandsgaard øe. présentées* le *19 décembre 2019, C-311/18, Data Protection Commissioner / Facebook Ireland et Maximillian Schrems,* §319. ↩

156. Art. 21*bis* et 61*ter* CICr. ↩

157. Art. 61*ter,* §3 CICr. ↩

158. Art. 39, §§1 à 3 de la loi du 30 juillet 2018. ↩

159. Art. 39, §3 de la loi du 30 juillet 2018. Selon le considérant 47 de la directive 2016/680, les méthodes visant à limiter le traitement de données à caractère personnel pourraient consister, entre autres, à déplacer les données sélectionnées vers un autre système de traitement à des fins archivistiques, ou à rendre les données sélectionnées inaccessibles ↩

160. Art. 39, §4 de la loi du 30 juillet 2018. ↩

161. Art. 42, al. 1 de la loi du 30 juillet 2018 ↩

162. Cour EDH, *M.K. c. France*, 18 avril 2013, § 44. Cette question devra être tranchée par la Cour de Justice de l'Union européenne, la Cour d'appel de Bruxelles ayant posé des questions préjudicielles sur ce point. (NBP : Bruxelles (civ.), 9 mai 2022, RG 2021/AR/983). ↩

163. Art. 646, al. 1 et 2 CICr. ↩

164. Art. 646, al. 3 CICr. ↩

165. Art. 646, al. 1 et 2 CICr. ↩

166. Selon les travaux préparatoires, l'arrêté royal visait justement à encadrer « le mode de transmission de ces données ainsi que la sélection des données pertinentes » (exposé des motifs du projet de loi modifiant la loi sur la fonction de police, la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *Doc. Parl.*, Ch., 2013–2014, DOC 53–3105/001, p. 75). ↩

167. Loi du 5 août 1992 sur la fonction de police, *M.B.*, 22 décembre 1992. ↩

168. C.O.C., *Rapport d'activité 2020*, *op. cit.,* p. 18. ↩