

AVIS

de l'AUTORITE DE CONTROLE JUDICIAIRE

créée par la loi du 1^{er} 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

sur l'application JUCHA

INTRODUCTION

L'autorité de contrôle judiciaire (ci-après « ACJ »), instituée par l'article 40 de la *loi du 1^{er} 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* (ci-après : la « loi du 1^{er} août 2018 en matière pénale ainsi qu'en matière de sécurité nationale ») transposant la *Directive (UE) 2016/680 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 des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil* (ci-après la « directive 2016/680 »), « 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 » conformément à l'article 42, paragraphe 1, lettre c) de ladite loi dans les limites de ses compétences prévues à l'article 40, paragraphe 2, à savoir en ce qui concerne les « opérations de traitement de données à caractère personnel effectuées par les juridictions de l'ordre judiciaire, y compris le ministère public, et de l'ordre administratif dans l'exercice de leurs fonctions juridictionnelles, que ce soit pour les finalités visées à l'article 1^{er} de la [loi du 1^{er} août 2018 en matière pénale ainsi qu'en matière de sécurité nationale] ou pour celles visées par le [règlement européen 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (ci-après le « RGPD »)] ».

Il ressort de l'article 1, paragraphe 1, conjointement avec l'article 40, paragraphe 2, de la loi du 1^{er} août 2018 en matière pénale ainsi qu'en matière de sécurité nationale que le ministère public est une autorité compétente au sens de ladite loi pour les « traitements de données à caractère personnel mis en œuvre à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces », en particulier pour les traitements de données découlant de l'application du Code pénal et du Code de procédure pénale et dans le respect des attributions des juridictions judiciaires, telles que découlant de la *loi modifiée du 7 mars 1980 sur l'organisation judiciaire*, effectués dans le contexte de la poursuite pénale.

Lesdites opérations de traitement de données, effectuées dans l'exercice des fonctions juridictionnelles du ministère public, sont « soumises au contrôle de l'autorité de contrôle judiciaire » conformément à l'article 40, paragraphe 2, de la loi du 1^{er} août 2018 en matière pénale ainsi qu'en matière de sécurité nationale.

Le présent avis vise à analyser l'application JUCHA au regard de la législation en matière de protection des données et s'appuie notamment sur des échanges entre l'ACJ et le Parquet général. L'avis est consacré à l'analyse de cet outil et ne concerne donc pas tous les traitements de données à caractère personnel mis en œuvre par les différentes juridictions répressives. Il convient d'emblée de préciser que cette analyse ne préjuge en rien l'adéquation de fait de la pratique et des procédures mises en place par l'administration judiciaire avec les exigences de la loi du 1^{er} août 2018 et du RGPD.

Le Parquet général met en œuvre l'application JUCHA qui est l'application interne pour la gestion centrale de l'ensemble des services de l'ordre judiciaire traitant les affaires pénales. Elle regroupe en une seule application l'essentiel des traitements informatisés, accessibles en tout ou partie, par les services de l'ordre judiciaire traitant les affaires pénales. Il s'agit d'une application de gestion de dossiers papier permettant de retracer l'emplacement physique desdits dossiers en créant une notice par dossier. Cette notice « JUCHA » contient en outre d'autres éléments sur le dossier papier, comme par exemple les personnes concernées (prévenus, victimes, tiers), les infractions visées et, actuellement de manière très limitée, les documents contenus dans le dossier.

L'application JUCHA couvre tout le processus d'une affaire pénale, depuis la communication du fait au parquet jusqu'à la décision définitive sur l'action publique, y compris l'inscription au casier judiciaire. Elle couvre encore le volet de l'exécution des peines. Par ailleurs, l'application JUCHA intègre la gestion des dossiers du Service central d'assistance sociale (ci-après « SCAS »), de la probation, de la tutelle, de la protection de la jeunesse, de l'aide aux victimes et des demandes de grâce.

Outre les traitements d'ores et déjà dématérialisés repris dans l'application JUCHA, il apparaît que celle-ci est appelée à évoluer, en intégrant au fur et à mesure davantage de dossiers dématérialisés liés à la mise en œuvre de l'« e-justice ». S'il est envisagé d'intégrer, à terme, une version dématérialisée des dossiers papier dans l'application JUCHA, les règles relatives à ladite application doivent couvrir également cette nouvelle réalité.

Eu égard à l'imbrication de multiples traitements de données au sein de l'application JUCHA s'appuyant en grande partie sur les mêmes données à caractère personnel collectées, cette analyse doit s'effectuer en distinguant les finalités. Quatre grandes catégories de finalités ont pu être identifiées :

A. La gestion du procès pénal

- a. Assurer la gestion des dossiers répressifs du premier acte de procédure jusqu'à l'exécution des décisions de justice,
- b. Permettre la gestion informatique des affaires pénales ouvertes au sein des parquets,
- c. Permettre aux procureurs d'Etat d'apprécier l'opportunité des poursuites,
- d. Permettre de retracer une affaire en cas de découverte d'éléments nouveaux,
- e. Permettre une gestion des audiences de nature répressive,
- f. Permettre la gestion du casier judiciaire avec les différents extraits,
- g. Gérer les dossiers du Service central d'assistance sociale (ci-après « SCAS ») (module SCAS).

B. La protection de la jeunesse

C. La coopération internationale en matière pénale et judiciaire

- a. Gérer et garder une trace des mandats d'arrêt européens et des autres instruments européens de reconnaissance mutuelle adressés au Luxembourg,
- b. Gérer et garder une trace des commissions rogatoires avec mesure de coercition adressées au Luxembourg.

D. Les autres missions des parquets

- a. Permettre la restitution d'objets retrouvés,
- b. Permettre aux procureurs d'État d'apprécier la moralité et l'honorabilité d'une personne,
- c. Garder une trace des dossiers papier transmis aux archives,
- d. Les interactions en dehors d'une procédure judiciaire en cours du parquet avec des personnes physiques ou morales.

Le fonctionnement actuel de l'application JUCHA est marqué par les différents textes législatifs et réglementaires qui ont encadré ladite application ainsi que les applications informatisées précédentes, comme la « chaîne pénale. ».

A titre de rappel, les traitements de données à caractère personnel informatisés mis en œuvre par les autorités judiciaires ont été encadrés dès l'entrée en vigueur de la *loi du 31 mars 1979 réglementant l'utilisation des données nominatives dans les traitements informatiques*, premier cadre législatif luxembourgeois relatif aux traitements de données informatisés, qui disposait, en son article 8, que « La création et l'exploitation de banques de données nominatives pour le compte de l'Etat ne peuvent se faire qu'en application d'une loi ou d'un règlement grand-ducal. ». Sur ce fondement, le *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*, tel que complété par le *règlement grand-ducal du 26 mars 1994 prorogeant l'autorisation d'exploiter la banque de données nominatives, dite chaîne pénale, au parquet de Luxembourg*, a constitué la première base légale de la « chaîne pénale », application informatique ayant précédé l'application JUCHA. Ces deux règlements grand-ducaux prévoyaient notamment des règles procédurales relatives à l'accès temporel et à l'accès fonctionnel à la banque de données et des règles relatives à la journalisation ainsi que des dispositions sur les données contenues dans la « chaîne pénale ». Le fonctionnement actuel de l'application JUCHA suit en grande partie la logique de ces deux instruments juridiques, même s'ils ne sont plus en vigueur.

L'article 8 de la *loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel*, entretemps abrogée et remplacée par la loi du 1^{er} août 2018 en matière pénale ainsi qu'en matière de sécurité nationale, remplaçait ces deux règlements grand-ducaux et précisait que :

« (1) Le traitement des données dans le cadre d'enquêtes pénales et de procédures judiciaires est opéré dans le respect des dispositions du Code de procédure pénale, du Code

de procédure civile, de la loi portant règlement de procédure devant les juridictions administratives ou d'autres lois.

(2) Le traitement de données relatives aux infractions, aux condamnations pénales ou aux mesures de sûreté ne peut être mis en œuvre qu'en exécution d'une disposition légale.

(3) Il ne peut être tenu de recueil exhaustif des condamnations pénales que sous le contrôle de l'autorité publique compétente en la matière. ».

Depuis l'entrée en vigueur de la loi du 1^{er} août 2018 en matière pénale ainsi qu'en matière de sécurité nationale, l'application JUCHA et les traitements de données à caractère personnel mis en œuvre par les autorités répressives sont encadrés par cette loi-cadre, sans contenir des dispositions spécifiques concernant les traitements de données mis en œuvre par les différentes autorités compétentes visées par ladite loi.

Il ne fait aucun doute que les traitements de données effectués par les autorités compétentes en matière pénale ainsi qu'en matière de sécurité nationale constituent une ingérence dans le droit au respect de la vie privée et le droit à la protection des données et que les dispositions pénales, en particulier le Code pénal et le Code de procédure pénale, constituent une base légale suffisante pour la collecte de données à caractère personnel dans l'exécution des missions essentielles du ministère public et des juridictions judiciaires.

Il convient cependant d'analyser si l'application JUCHA ne constitue pas un traitement de données distinct, et allant au-delà, des traitements de données basés sur les procédures pénales décrites ci-dessus, en ce qu'elle facilite l'exploitation et la mise en relation d'informations sur la base de procédures judiciaires distinctes et permet des rapprochements entre ces différents traitements de données ayant des finalités connexes, de sorte que les conditions et les modalités de ce traitement de données « JUCHA » devraient être prévues dans la loi afin de conférer une plus grande sécurité juridique aux justiciables.

Il est à noter que les dispositions légales citées restent muettes sur les caractéristiques principales des traitements effectués à travers l'application JUCHA. Cette application est dès lors à ce stade encadrée par la seule loi-cadre, la loi du 1^{er} août 2018 en matière pénale ainsi qu'en matière de sécurité nationale.

Ainsi, il convient d'analyser si les dispositions de ladite loi sont suffisamment précises quant aux exigences en particulier de l'article 11, paragraphe 3, lu à la lumière l'article 32, paragraphe 3, de la Constitution, de l'article 8, paragraphe 2, de la Convention européenne des droits de l'homme, de l'article 52, paragraphes 1 et 2, de la Charte des droits fondamentaux de l'Union européenne et de la jurisprudence s'y référant.

A cet égard, il convient de s'interroger si les traitements de données effectués à travers l'application JUCHA ne constituent pas une ingérence dans la vie privée des citoyens supplémentaire à l'ingérence, nécessaire dans une société démocratique, des dispositions pénales dans les droits et libertés fondamentales prévus par la loi, et différente de celle-ci, et ne nécessiteraient pas un encadrement législatif distinct. Une ingérence dans le droit au respect de la vie privée ou dans le droit à la protection des données peut être justifiée à condition qu'elle :

A. soit prévue par une loi accessible aux personnes concernées et prévisible quant à ses répercussions, c'est-à-dire formulée avec une précision suffisante ;

- B. soit nécessaire dans une société démocratique, sous réserve du principe de proportionnalité ;
- C. respecte le contenu essentiel du droit à la protection des données ;
- D. réponde effectivement à des objectifs d'intérêt général ou au besoin de protection des droits et libertés d'autrui.

La jurisprudence de la Cour européenne des droits de l'homme (ci-après « CEDH ») et celle de la Cour de justice de l'Union européenne (ci-après « CJUE ») soulignent l'importance de la précision et de l'accessibilité pour « fournir à l'individu une protection adéquate contre l'arbitraire »¹ et offrir des « garanties suffisantes permettant de protéger efficacement leurs données à caractère personnel contre les risques d'abus ainsi que contre tout accès et toute utilisation illicites de ces données. »².

De plus, au regard de l'article 11, paragraphe 3, de la Constitution, lu ensemble avec l'article 32, paragraphe 3, de la Constitution, et de la jurisprudence de la Cour constitutionnelle³, les éléments essentiels, les objectifs et les principes doivent figurer dans la loi au sens strict du terme en ce qui concerne les limitations à la protection de la vie privée.

La loi du 1^{er} août 2018 en matière pénale ainsi qu'en matière de sécurité nationale précise les règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel qui sont à respecter par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces. L'article 8 de la directive 2016/680 dispose que pour être licite, le traitement doit être nécessaire à l'exécution d'une mission de l'autorité compétente, correspondre aux finalités pour lesquelles il a été mis en place, mais aussi et surtout, il doit être prévu soit par le droit de l'Union, soit par le droit national.

En amont du présent avis, l'ACJ, appuyée par un expert technique, a échangé avec le parquet général au sujet du fonctionnement u dans le contexte de cette analyse. Les documents de référence qui ont été échangés dans ce contexte sont également repris.

¹CEDH, arrêt (plénière, au principal) du 2 août 1984, *Malone c. Royaume-Uni*, 8691/79, série A n° 82, pp. 31-32, ECLI:CE:ECHR:1984:0802JUD000869179, § 66.

²CJUE, arrêt (grande chambre) du 8 avril 2014, *Digital Rights Ireland Ltd contre Minister for Communications, Marine and Natural Resources e.a. et Kärntner Landesregierung e.a.*, affaires jointes C 293/12 et C 594/12, ECLI:EU:C:2014:238, point 54.

³Voir notamment: Cour constitutionnelle, arrêt du 2 mars 2018, n° 132/18, Mém. A n° 196 du 20 mars 2018 ; Cour constitutionnelle, arrêt du 2 mars 2018, n° 133/18, Mém. A n° 197 du 20 mars 2018.

Date	Événement
14/10/2019	L'ACJ transmet le questionnaire 1 au Parquet général
29/11/2019	Réponse du Parquet général au questionnaire 1
06/12/2019	Le Parquet général transmet l'étude d'impact
09/01/2020	L'ACJ transmet le questionnaire 2 au Parquet général et formule une demande de réunion
24/01/2020	Réponse du Parquet général au questionnaire 2
03/02/2020	Réunion entre l'ACJ, le Parquet général et l'expert technique, comportant une démonstration de l'application JUCHA
12/02/2020	Transmission de documents par le Parquet général suite à la réunion du 3 février 2020
14/07/2020	Réponse du Parquet général à des questions complémentaires (mises à jour)

Le présent avis est structuré comme suit :

A. Analyse technique de l'application JUCHA.....	7
B. Caractéristiques générales des traitements de données effectués dans l'application JUCHA.....	10
C. Les durées de conservation et la gestion des accès.....	14
D. Les mesures de sécurité.....	21
E. Conclusion.....	26

A. ANALYSE TECHNIQUE DE L'APPLICATION JUCHA

L'application JUCHA est construite et organisée sur base du « numéro de notice JUCHA » attribué à une affaire donnée, au moment de sa saisie initiale et qui reste inchangé durant toute la procédure. En principe un dossier (c'est-à-dire une affaire) est ouvert par un des deux parquets auprès des tribunaux d'arrondissement de Luxembourg et de Diekirch ou plus rarement par un des cabinets d'instruction auprès des deux tribunaux, qui y inscrivent alors l'ensemble des données disponibles au moment de la création du numéro de référence « JUCHA ». Par la suite, les données additionnelles sont inscrites par le service qui les reçoit ou les génère. Au vu des compétences spéciales qui sont les leurs, les juridictions de la jeunesse peuvent également créer une référence « JUCHA » relative à un dossier en matière de protection de la jeunesse. De même, le SCAS peut créer ses propres dossiers et références « JUCHA » correspondantes. Les références en matière de protection de la jeunesse ainsi que celles du SCAS sont cependant séparées des notices JUCHA proprement dites et ne sont accessibles qu'aux personnes ayant les droits informatiques afférents, droits qui peuvent, par ailleurs, exister indépendamment du droit de consulter les notices en matière pénale.

Par la suite, la notice « JUCHA » est alimentée par des données venant des parquets, des juges d'instruction, de la chambre du conseil et des chambres correctionnelles et criminelles des tribunaux d'arrondissement, du Parquet général, de la chambre du conseil et des chambres correctionnelles et criminelles de la Cour d'appel ainsi que de la Cour de cassation.

Un aperçu quantitatif concernant le nombre de personnes inscrites dans JUCHA depuis 2009 (archivées et non-archivées – toutes notices confondues) au 29 juin 2020 se présente comme suit :

- personnes visées dans un mandat d'arrêt européen : 491
- personnes morales (« PM ») : 55 858
- personnes physiques (« PP ») : 665 967
dont (PM et PP) :
 - prévenus / inculpés : 349 896
 - parties civiles : 16 418
 - témoins : 63 186
 - l'Etat, les compagnies d'assurances, les victimes, les autres intervenants dans les procédures pénales et les autres personnes visées aux communications et rapports adressés aux procureurs d'Etat : 460 710.

Ces chiffres n'indiquent pas combien de personnes distinctes figurent dans l'application JUCHA. En effet, une personne peut revêtir plusieurs rôles dans un procès (p.ex. victime qui se déclare partie civile). De même, certains intervenants sont, à l'instar des compagnies d'assurance et de l'Etat, repris de nombreuses fois, à savoir dans chaque nouvelle notice qui les concerne. Enfin, une personne soupçonnée dans plusieurs affaires séparées est également reprise à chaque fois comme nouvelle personne (conséquence de l'absence de fichier basé sur les personnes). Pour la même raison, la somme des chiffres détaillés ne correspond pas à la somme des personnes (PM + PP) reprises dans l'application JUCHA.

Les recherches dans l'application JUCHA peuvent se faire sur base de personnes ou sur base d'affaires. Les critères de recherche suivants sont disponibles :

- personne : Date de naissance, Nom, Prénom, Matricule, Sexe, Localité, Inscriptions existantes (date de décisions , numéro de décision, date du fait), Exécution des peines (Type), Contrôle judiciaire (statut)
- affaire : No. Notice (Format: Numéro/année/Type) ou Numéro, Mot clé (Champ « Remarques », page d'accueil), Nom d'une partie, un numéro de PV, une référence Police, un numéro de jugement, Période des faits reprochés

A part un nombre limité de documents sous format électronique accessibles via l'application JUCHA, celle-ci vise la gestion électronique et purement administrative de plus de 60.000 nouveaux dossiers par an. L'application JUCHA ne remplace ainsi pas le dossier physique version papier. Voici quelques chiffres pour illustrer le nombre de notices « JUCHA » :

- 2009 nouvelles affaires: 49 434
- 2019 nouvelles affaires: 59 642
- nouvelles affaires créées depuis 2009 : 494 322
- taux des affaires archivées par rapport à celles qui sont encore ouvertes : 2/3

Les chiffres présentés reprennent uniquement les délits et les crimes et excluent les contraventions en raison du très grand nombre de contraventions au Code de la route qui « fausseraient » les statistiques.

« JUCHA-historique » est une sous-application de JUCHA et correspond à la partie « historique » de l'ancienne « chaîne pénale ». Elle reprend l'ensemble des inscriptions relatives :

- à des personnes prévenues, inculpées et/ou condamnées du chef d'une infraction pénale,
- aux autres personnes concernées par une telle infraction, notamment les victimes et d'autres intervenants concernés (p.ex. l'État, les compagnies d'assurances)
- aux personnes visées aux communications et rapports adressés aux procureurs d'Etat.

L'accès à « JUCHA-historique » est réservé aux magistrats des parquets et du Parquet général. Aucun accès n'est attribué aux juridictions du fond, afin de ne pas influencer sur leur décision : seul le casier judiciaire (bulletin 1) fait partie du dossier à la disposition du tribunal.

L'application JUCHA a été mise en production pour la première fois en 2007 pour ce qui est de la gestion numérique du casier judiciaire, la version finale a été mise en production pour tous les intervenants en 2009. Une « release note » est créée à chaque mise en production, permettant d'indiquer les améliorations et évolutions livrées ainsi que les éventuels correctifs mis en place.

Les acteurs suivants sont impliqués dans la gestion quotidienne de l'application :

- Service informatique de la Justice (« SIJ »),
- Comité directeur informatique (Ministère de la Justice, Parquet général, CTIE, SIJ),
- Co-contractant externe,
- Magistrats et personnel administratif.

L'application JUCHA est hébergée auprès du Centre des technologies de l'information de l'Etat (CTIE).

Au sujet des interfaces, l'application JUCHA utilise les services web suivants :

- RNPP : Utilisation du service RNPP pour la création et la mise à jour dans JUCHA des personnes physiques,
- Police (e-PV/CSA) : réception des procès-verbaux en format électronique afin de faciliter l'encodage d'une nouvelle affaire dans JUCHA, en complément à l'envoi de la version papier, retour d'informations sommaires vers la Police grand-ducale sur le suivi du dossier,
- ENRAM : Envoi des amendes à payer à l'Administration de l'enregistrement, des domaines et de la TVA (« AED ») pour recouvrement,
- JUIEX : Consultation de la base de données commune de toutes les applications métiers de la justice contenant les données des différents intervenants externes de la justice (avocats, notaires, huissiers, traducteurs et experts),
- ECRIS : European Criminal Records Information System, webservice d'échange de données judiciaires entre les pays de l'Union européenne.

Les services suivants sont mis à disposition des tiers par l'application JUCHA :

- MyGUICHET: Demande de casier judiciaire via le portail Guichet.lu (accès sur demande) pour une ou plusieurs personnes physiques. Cette demande peut émaner d'une personne physique ou morale en vue d'obtenir son propre casier (bulletins 3, 4 et 5). Elle peut encore émaner d'une des entités légalement autorisées à se voir communiquer un extrait du bulletin 2 ou du bulletin 3 en vertu de la *loi modifiée du 29 mars 2013 relative à l'organisation du casier judiciaire*. Dans le second cas, les extraits du casier sont envoyés sous format pdf individuel en cas de casier positif, après un contrôle humain (mécanisme semi-automatique). Les informations sur les casiers néants sont retournés auxdites entités sur une liste groupée. Un web-service a été mis en place pour certaines administrations de l'Etat qui permet la demande d'un casier sans passer par MyGUICHET dans une première phase. Dans cette configuration, les administrations reçoivent sur communication du matricule national via leur application métier (donc automatiquement), et de l'accord du concerné, l'information de l'existence ou de l'absence d'inscriptions au casier. Dans le cas d'un casier positif, la demande et la délivrance se feront toutefois par MyGUICHET et via un agent de l'administration concernée.
- ERRU : application à l'étude dans le cadre de la transposition du règlement d'exécution (UE) 2017/2205 de la Commission du 29 novembre 2017 relatif aux règles détaillées concernant les procédures de notification des véhicules utilitaires présentant des défaillances majeures ou critiques décelées lors d'un contrôle technique routier.

B. CARACTERISTIQUES GENERALES DES TRAITEMENTS DE DONNEES EFFECTUES DANS L'APPLICATION JUCHA

Le responsable du traitement pour l'application JUCHA

L'article 20 de la loi du 1^{er} août 2018 en matière pénale ainsi qu'en matière de sécurité nationale prévoit que, lorsque deux responsables du traitement ou plus déterminent conjointement les finalités et les moyens du traitement, ils sont les responsables conjoints du traitement.

Dans son avis relatif au projet de loi de transposition de la directive 680/2016 rendu en 2017, le Parquet général a estimé, au sujet de la détermination du responsable du traitement, qu'« *Il y a lieu de relever que de nombreuses banques de données, telles que JUCHA (chaîne pénale), sont alimentées par plusieurs acteurs : les parquets, les juges d'instruction, la chambre du conseil et les chambres correctionnelles et criminelles des tribunaux d'arrondissement, le Parquet général, la chambre du conseil et les chambres correctionnelles et criminelles de la Cour d'appel. Il serait faux de dire que le Parquet général, en tant que responsable du traitement, serait 'seul maître à bord'.* ». Dans ce même avis, le Parquet général a néanmoins estimé être le responsable du traitement pour l'application JUCHA⁴.

Comme le souligne le Parquet général, aux termes de l'article 3, paragraphe 8, de la loi du 1^{er} août 2018 en matière pénale ainsi qu'en matière de sécurité nationale, un responsable du traitement est « l'autorité compétente qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel » et le Parquet général apparaît comme le responsable de traitement en ce qui concerne l'application JUCHA.

Néanmoins, il n'est pas clair quel rôle chaque acteur joue dans le fonctionnement de l'application JUCHA. On peut s'interroger si les différentes juridictions ne devraient pas être considérées comme responsables de traitement conjoints, au moins pour certaines parties des traitements de données reprises dans l'application JUCHA.

Sous-traitance

L'application JUCHA est hébergée auprès du Centre des technologies de l'information de l'Etat et une entreprise privée est chargée par contrat conclu avec le CTIE de la maintenance technique et évolutive de JUCHA.

En vertu de l'article 21, paragraphe 1, de la loi du 1^{er} août 2018 en matière pénale ainsi qu'en matière de sécurité nationale, le responsable du traitement ne doit, dans le choix de sous-traitants, recourir qu'à ceux qui présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière que le traitement réponde aux exigences de la loi et garantisse la protection des droits de la personne concernée.

⁴ Avis du Parquet général portant sur le projet de loi 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, Doc. Parl. 7168/2, p. 19.

Par ailleurs, en vertu de l'article 21, paragraphe 3, de la prédite loi, le traitement par un sous-traitant doit être régi par « *un contrat ou un autre acte juridique au titre du droit de l'Union européenne, du droit luxembourgeois ou du droit d'un autre État membre, qui lie le sous-traitant à l'égard du responsable du traitement et qui définit l'objet et la durée du traitement, la nature et la finalité du traitement, le type de données à caractère personnel et les catégories de personnes concernées et les obligations et les droits du responsable du traitement.* ». Ledit acte doit prévoir que le sous-traitant respecte certaines règles, comme n'agir que sur instruction du responsable du traitement, veiller à ce que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité.

Les catégories et les sources des données à caractère personnel

Chaque affaire contient notamment les informations suivantes :

- personnes concernées (prévenu, victimes, tiers, ...),
- procès-verbaux et rapports de police/douane/ITM et autres OPJ/APJ,
- infractions,
- biens saisis,
- frais de justice,
- fixations à des audiences,
- décisions rendues par les juridictions d'instruction et de fond,
- mots-clés et autres éléments techniques (Champ « Remarques », page d'accueil).

Pour chaque personne apparaissant dans une affaire en tant qu'inculpée, prévenue ou condamnée, les informations suivantes sont conservées :

- informations signalétiques,
- éventuelles détentions,
- différentes peines (peines privatives de liberté, amendes, retraits de permis, peines accessoires ...).

Pour toute personne condamnée, les données nécessaires (i.e. données signalétiques et détails des condamnations définitives) sont encore reprises dans son casier judiciaire. Pour les autres personnes sont conservées seules les données signalétiques nécessaires pour leur rôle spécifique dans la procédure concernée. L'application JUCHA contient encore les données relatives aux noms, prénoms et fonctions des magistrats (magistrature debout et assise) intervenus dans une affaire.

Finalement, certains documents sont contenus dans l'application JUCHA :

- les procès-verbaux, dits « e-pvs » (transmission de certains PV par voie électronique avant envoi sous forme papier, la loi ne prévoyant pas encore une transmission uniquement sous forme digitale),
- les photos transmises par la Police grand-ducale via le même canal dans le cadre des dossiers d'excès de vitesse constatés par les systèmes de contrôles automatisés (CSA/radars) donnant lieu à une procédure judiciaire.

L'application contient encore les documents suivants :

- les dossiers d'entraide pénale internationale, y compris les décisions d'enquête européennes
- les dossiers se basant sur certains instruments européens relatifs à la reconnaissance mutuelle (mandats d'arrêt européens, ...).

Ces dossiers, figurant dans des modules spécifiques de JUCHA, ne sont cependant accessibles qu'aux seules personnes amenées, de par leur fonction, à traiter des affaires en matière d'entraide pénale, à savoir un nombre limité de magistrats du ministère public, les juridictions d'instruction (juges d'instruction et chambres du conseil) et un nombre fortement limité du personnel administratif.

Eu égard aux finalités poursuivies, les données à caractère personnel reprises dans l'application JUCHA ne semblent pas disproportionnées par rapport aux principes découlant notamment de l'article 3, paragraphe 1, lettre c) de la loi du 1^{er} août 2018 en matière pénale ainsi qu'en matière de sécurité nationale qui précise que les données à caractère personnel visées par la loi sont adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont traitées.

Toutefois, dans l'optique d'accroître la prévisibilité de la loi et de garantir ainsi un degré de sécurité juridique accru pour les citoyens, il serait recommandé d'encadrer, par une disposition légale, la diversité des sources qui alimentent l'application JUCHA ainsi que la pluralité des destinataires des données.

Le traitement de données à caractère personnel contenues dans les documents introduits sous format électronique se base en principe sur le même fondement légal que le traitement de ces données en version papier. Toutefois, étant donné les évolutions techniques à prévoir (projet e-Justice), il convient de s'interroger si le traitement systématique de documents liés à la procédure pénale dans l'application JUCHA ne devrait pas davantage être encadré par une disposition légale afin de prendre pleinement en compte l'article 7 de la loi du 1^{er} août 2018 en matière pénale ainsi qu'en matière de sécurité nationale, en particulier lorsqu'il s'agit d'entreprendre des opérations de traitement de données allant au-delà d'une simple gestion administrative de dossier. Une telle démarche proactive pourrait en même temps permettre d'anticiper d'éventuelles finalités ou traitements de données envisageables avec la mise en place de la digitalisation de la « justice pénale » dans un proche avenir.

La distinction entre différentes catégories de personnes concernées

L'article 5 de la loi du 1^{er} août 2018 en matière pénale ainsi qu'en matière de sécurité nationale pose l'exigence suivante : « Le responsable du traitement établit, le cas échéant et dans la mesure du possible, une distinction claire entre les données à caractère personnel de différentes catégories de personnes concernées, telles que :

- les personnes à l'égard desquelles il existe des motifs sérieux de croire qu'elles ont commis ou sont sur le point de commettre une infraction pénale ;
- les personnes reconnues coupables d'une infraction pénale ;
- les victimes d'une infraction pénale ou les personnes à l'égard desquelles certains faits portent à croire qu'elles pourraient être victimes d'une infraction pénale, et
- les tiers à une infraction pénale, tels que les personnes pouvant être appelées à témoigner lors d'enquêtes en rapport avec des infractions pénales ou des procédures pénales ultérieures, des personnes pouvant fournir des informations sur des infractions pénales, ou des contacts ou des associés de l'une des personnes visées aux lettres a) et b). ».

En pratique, l'application JUCHA semble respecter cette disposition, en ce qu'elle fait la distinction entre les personnes physiques suivantes :

- personnes visées dans un mandat d'arrêt européen,
- prévenus / inculpés,
- parties civiles,
- témoins,
- victimes.

Toutefois, il convient de clarifier quelles différences de traitement s'attachent à cette distinction, notamment en ce qui concerne la possibilité d'effectuer une recherche sur lesdites personnes et les informations affichées en fonction des différentes catégories de personnes.

C. LES DUREES DE CONSERVATION ET LA GESTION DES ACCES

Considérations générales en matière de gestion des durées de conservation

Pour les raisons exposées ci-dessous concernant la gestion du procès pénal et des archives définitives des services de l'ordre judiciaire traitant les affaires pénales, les dossiers répressifs et les informations y relatives sont conservés sans limitation de temps dans l'application JUCHA étant entendu que la visibilité des informations diminue en fonction de l'ancienneté des inscriptions, tel que décrit ci-après. Par conséquent, en parallèle à l'analyse des durées de conservation, il est primordial de s'interroger sur une politique d'accès afin de respecter les principes de proportionnalité et de nécessité, le principe de minimisation, découlant de l'article 3 de la loi du 1^{er} août 2018 en matière pénale ainsi qu'en matière de sécurité nationale, ainsi que le principe de « privacy by design et by default » au sens de l'article 19 de la prédite loi.

L'article 4 de la loi du 1^{er} août 2018 en matière pénale ainsi qu'en matière de sécurité nationale prévoit que le responsable de traitement « fixe des délais appropriés pour l'effacement des données à caractère personnel ou pour la vérification régulière de la nécessité de conserver les données à caractère personnel » et « établit des règles procédurales en vue d'assurer le respect de ces délais qui déterminent les personnes intervenant au nom et pour compte du responsable du traitement dans cette procédure ». Néanmoins, en confiant la responsabilité de la fixation des délais de conservation à chaque responsable du traitement, il semble que le législateur luxembourgeois ait interprété de manière trop extensive la marge de manœuvre consentie par l'article 5 de la directive (UE) 2016/680, en ce que cette disposition laisse le soin aux Etats membres et non au responsable du traitement des données de fixer des délais appropriés pour l'effacement des données à caractère personnel et la vérification de la nécessité de conserver lesdites données.

L'article 5 de la Directive (UE) 2016/680 prévoit ce qui suit :

« Les États membres prévoient que des délais appropriés sont fixés pour l'effacement des données à caractère personnel ou pour la vérification régulière de la nécessité de conserver les données à caractère personnel. Des règles procédurales garantissent le respect de ces délais. ».

Au sujet de la transposition de cette disposition, en estimant que « la directive [laisse], sur ce point, toute liberté au législateur », le Conseil d'Etat a indiqué avoir

« [...] une nette préférence pour la solution qui consiste à prévoir dans la loi la possibilité pour le responsable du traitement de fixer tant les délais prévus pour l'effacement des données que ceux prévus pour la vérification de la nécessité de conserver lesdites données, ce qui visera les données pour lesquelles, notamment pour des raisons tenant à la procédure pénale, des délais précis ne peuvent pas être imposés par la loi. »⁵.

⁵ Avis du Conseil d'Etat du 29 mai 2018 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, Doc. Parl. 7168/8, p. 10.

En revanche, la Commission nationale pour la protection des données a estimé ce qui suit :

« La CNPD est cependant d'avis qu'il n'appartient pas au responsable du traitement (c'est-à-dire la Police Grand-ducale, le Service de renseignement de l'Etat, l'Administration des douanes et accises etc.) de fixer les délais de conservation des données, mais qu'il revient au législateur de les fixer.

Des lois spéciales devront fixer, de manière précise, la durée de conservation pour chaque traitement de données tout comme elles devront prévoir l'existence même des différents traitements de données.»⁶.

Par ailleurs, 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.

Eu égard au caractère extrêmement sensible d'un traitement de données relatives à l'implication d'individus dans une affaire pénale, même aux accès strictement limités, il serait d'autant plus approprié de fixer les durées de conservation ou du moins les critères applicables pour déterminer les durées par un texte légal.

En considération, d'un côté, de la multiplicité des finalités dont certaines dépassent le cadre de la gestion des affaires pénales (comme par exemple le contrôle de l'honorabilité ou de la moralité lors de recrutements) et, d'un autre côté, du fait que des données qui ne se trouvent plus dans la partie active ne sont pas effacées, mais restent dans la partie archives dont les conditions d'accès sont plus restrictives, on pourrait songer à un système dans lequel la durée d'accès serait individualisée en fonction de la finalité poursuivie au moment d'une consultation. Le magistrat ou un autre agent devrait ainsi, au moment de la consultation, introduire le motif pertinent pour pouvoir accéder aux données.

La catégorie d'infractions (contraventions, délits, crimes) peut être un critère pour la détermination du délai de conservation étant donné que le délai de prescription en dépend.

Dès lors, sans préjuger du caractère adéquat de la pratique mise en place au sein du Parquet général, il convient de s'interroger si, à la lumière des développements présentés, les durées de conservation et la politique d'accès font partie des éléments essentiels, des objectifs et des principes d'un traitement de données en matière pénale qui devraient être définis par une disposition légale.

⁶ 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, Doc. Parl. 7168/4, pp. 1-2.

La gestion du procès pénal

Les règles de procédure définissent en grande partie les délais de conservation, y compris dans l'application JUCHA, et sont définies par le Code de procédure pénale, le Code pénal et la *loi modifiée du 7 mars 1980 sur l'organisation judiciaire* pour les finalités liées à la gestion du procès pénal, à savoir :

- assurer la gestion des dossiers répressifs du premier acte de procédure jusqu'à l'exécution des décisions de justice,
- permettre de retracer une affaire en cas de découverte d'éléments nouveaux,
- permettre une gestion des audiences en matière pénale,
- permettre la gestion du casier judiciaire avec les différents extraits,
- gérer les dossiers SCAS (module SCAS).

La durée de conservation des données à caractère personnel en matière pénale est influencée par les délais de prescription de l'action publique et des peines (articles 635 et suivants du Code de procédure pénale). De même, pour les dossiers dans lesquels il y a condamnation, il convient de noter que le droit à la révision (articles 443 et suivants du Code de procédure pénale) implique que toute personne condamnée, ainsi que ses descendants, aient le droit, dans des conditions particulières, de demander la révision. Afin de garantir ce droit et le respect de toutes les parties au procès, l'accès au dossier pénal doit être assuré en tout temps. Toutefois, en prenant en compte le caractère exceptionnel de cette procédure ainsi que le nombre restreint de personnes pouvant l'initier, une politique d'accès restrictive semble adaptée à cette finalité. La pratique actuelle semble refléter cette mise en balance des droits.

L'action publique faisant partie des fonctions régaliennes de l'Etat, la quasi-intégralité des dossiers pénaux est, à terme, vouée à un archivage définitif au sens de la loi du 17 août 2018 relative à l'archivage. Par conséquent, étant donné que les juridictions judiciaires conservent et gèrent elles-mêmes les archives publiques au sens de l'article 4 de ladite loi et que l'application JUCHA est également utilisée pour la gestion de ces archives définitives, les notices JUCHA sont, en pratique, conservées indéfiniment.

En pratique, d'une manière générale, une affaire est « archivée » dans l'application JUCHA si le dossier matériel est archivé à son tour. A défaut, le dossier est « archivé » dans l'application JUCHA après deux ans pour les affaires de police et après trois ans pour les affaires criminelles et correctionnelles après le dernier événement ou la dernière décision intervenue dans un dossier.

- Le délai de deux ans pour les affaires de police (contraventions et délits décorrectionnalisés) tient compte de la moindre gravité de ces faits, du délai de prescription d'un an pour les contraventions et du délai de prescription des peines en matière contraventionnelle qui est de deux ans.
- Les trois ans correspondent au délai de prescription des délits avant 2009. Une adaptation de ce délai à une période de cinq ans, qui correspondrait au délai de prescription des délits actuel, ne s'est pas encore imposée, mais une réflexion est en cours sur ce point.

Une évolution de l'application JUCHA tendant à limiter la visibilité de l'existence même des affaires « archivées » est actuellement en place depuis la mise en production de la version 4.1.2 du 28 janvier 2020 (disparition de l'affichage à l'écran d'un dossier archivé cinq ans après la date d'archivage, sauf pour des personnes nommément désignées).

Actuellement, aucune donnée enregistrée dans JUCHA n'est effacée, mais les données sont archivées après un certain temps. Un effacement des données aurait notamment comme conséquence une impossibilité de gestion des archives des dossiers matériels qui ne sont pas détruits, mais transmis pour conservation aux Archives nationales. Par ailleurs, il s'impose de pouvoir recourir à ces données, même archivées, dans le cadre de certaines procédures (révision, faits nouveaux dans des affaires non-encore prescrites, ...), mais également pour assurer le droit des victimes (p.ex. restitution d'objets retrouvés longtemps après les faits, ...). A noter que, contrairement à la prescription en matière pénale, la prescription civile de droit commun est de 30 ans, de telle sorte qu'une victime pourra être dans l'obligation de recourir au contenu d'un dossier pénal même longtemps après l'archivage de ce dernier dans l'application JUCHA si elle entend faire valoir ses droits devant un juge civil.

Il semble, dès lors, que trois phases soient à distinguer :

- phase « active » du dossier pénal, lorsque la notice JUCHA et son contenu sont visibles à la plupart des utilisateurs JUCHA, en fonction du profil d'accès attribué,
- phase « passive » du dossier pénal, après les délais indiqués (en principe trois ans), lorsque l'existence d'une notice JUCHA est affichée et que son contenu est uniquement accessible à un nombre restreint de personnes ou sur demande,
- phase « archivée » du dossier pénal, lorsque l'existence d'une notice JUCHA n'est visible qu'à un nombre encore plus restreint de personnes (en principe uniquement le chef d'administration, le Procureur général d'Etat et ses représentants) en fonction de besoins spécifiques.

Dans tous les cas, il convient de souligner que l'accès à une notice JUCHA est strictement encadré et doit être justifié par un besoin de service, ainsi qu'il sera précisé ci-après.

Les délais d'accès, pour les besoins de gestion du procès pénal, ne semblent pas disproportionnés et l'approche retenue d'un accès modulé semble s'aligner avec les principes de protection des données par défaut et par design étant donné, comme il sera analysé plus loin, que cet accès est revu périodiquement en fonction des besoins des différents profils d'accès, basés sur le principe du « need-to-know », et que le statut d'une notice JUCHA s'adapte également progressivement, en cas d'inactivité dans un dossier, aux finalités poursuivies.

L'opportunité des poursuites

Une des finalités de l'application JUCHA est de permettre aux procureurs d'Etat d'apprécier l'opportunité des poursuites. L'application JUCHA semble être utilisée pour retracer l'historique d'une personne, y compris les affaires pénales qui n'ont pas abouti à un procès pénal. A cet égard, il peut être pertinent de s'interroger sur la proportionnalité de cette utilisation des données issues de l'application JUCHA, en particulier lorsqu'il s'agit de notices JUCHA relatives à des affaires ayant fait l'objet d'une décision de non-lieu ou de classement sans suites, étant entendu qu'une décision de non-lieu n'entraîne pas une extinction de l'affaire pénale alors qu'au vu des articles 135 et suivants du Code de procédure pénale, l'instruction peut être reprise en cas de découverte de charges nouvelles. De même le classement sans suites constitue une simple mesure administrative, par nature provisoire, qui peut être reconsidérée tant que la prescription n'est pas acquise. Il s'agit d'une appréciation relevant des critères de l'action répressive dans le cadre de laquelle il devra être examiné à partir de quel moment une affaire ne devrait en général plus entrer en ligne de compte pour apprécier l'opportunité des poursuites, en fonction de la gravité des faits d'affaires précédentes et de l'affaire pour laquelle l'opportunité des poursuites est à apprécier. Si le législateur entend légiférer, dans ce domaine, sur la durée de conservation, il devra tenir compte des exigences liées à l'indépendance du ministère public dans le cadre de l'opportunité des poursuites.

La protection de la jeunesse

Les autorités judiciaires chargées de l'application de la *loi modifiée du 10 août 1992 relative à la protection de la jeunesse* utilisent également une partie dédiée de l'application JUCHA, sans que les mêmes règles soient pour le moment applicables aux délais.

En matière de jeunesse, il existe à travers l'application JUCHA, d'une part, la consultation des dossiers jeunesse et, d'autre part, la consultation du registre spécial jeunesse prévu par l'article 15 de la *loi modifiée du 10 août 1992 relative à la protection de la jeunesse*.

En pratique, les dossiers jeunesse sont accessibles uniquement à travers la fonction « *recherche d'affaires jeunesse* », à laquelle seulement un nombre limité de magistrats et de personnel administratif ont accès. Chaque dossier se rapporte à toute la fratrie maternelle et concerne ainsi, dans la plupart des cas, respectivement plusieurs mineurs et des enfants devenus entretemps majeurs. Dans chaque dossier jeunesse figure le relevé de tous les documents (rapports sociaux, décisions judiciaires, procès-verbaux de la police, etc.) qui se trouvent versés au dossier matériel. Un archivage n'est actuellement pas prévu, mais est à l'étude. Les décisions de principe, tenant compte de la spécificité du droit de la protection de la jeunesse quant à la durée de conservation, ont d'ores et déjà été prises. Elles doivent toutefois, avant d'être mises en œuvre, être examinées au niveau de la faisabilité technique.

Pour ces dossiers jeunesse, qui concernent à chaque fois toute une fratrie maternelle et donc souvent plusieurs mineurs, il est envisagé de mettre en place le même délai de base de trois ans avant d'archiver. Ce délai prendra cours à la dernière des dates, soit celle de la majorité de l'enfant le plus jeune de la famille suivie soit, en cas de décision de prolongation prise

conformément aux articles 1,3,4, ou 5 de la *loi modifiée du 10 août 1992 relative à la protection de la jeunesse*, celle de l'expiration de cette prolongation.

En pratique, pour le registre spécial jeunesse tel que prévu par l'article 15 de la loi modifiée du 10 août 1992 relative à la protection de la jeunesse, et qui est accessible à travers la fonction « *recherche personne* » à laquelle tous les utilisateurs de JUCHA ont accès, un archivage est en train d'être instauré. Ce registre ne contient que le dispositif des seules décisions judiciaires (mesures de garde, jugements). Etant donné que le registre de la jeunesse est expressément prévu à l'article 15 de la prédite loi, celle-ci doit être adaptée pour que ce délai d'archivage, qui sera dès à présent instauré sur une base informelle, puisse être consacré dans une base légale suffisante.

Ainsi, comme il est déjà prévu en pratique, il convient d'apprécier la nécessité d'adapter la législation relative à la protection de la jeunesse ou de veiller à ce que le projet de loi en cours en cette matière prenne dûment en compte les exigences décrites ci-dessus. Il convient plus particulièrement de séparer dans l'application JUCHA jeunesse les documents relatifs à la protection de la jeunesse (p.ex. enquête sociale) qui concernent effectivement toute la fratrie, des documents relatifs à des faits fautifs reprochés au mineur qui sont susceptibles de constituer une infraction d'après la loi pénale (p.ex. procès-verbal de police, décision de justice) qui ne concernent en principe qu'une seule personne et dont l'accès devrait être limité à une consultation visant un individu en particulier.

La coopération internationale en matière pénale et judiciaire

Pour les affaires liées à la coopération internationale en matière pénale et judiciaire, il semble que la pratique actuelle d'archivage, ayant pour finalités notamment de « gérer et garder une trace des mandats d'arrêt européens et des autres instruments européens de reconnaissance mutuelle adressés au Luxembourg » et de « gérer et garder une trace des commissions rogatoires avec mesure de coercition adressées au Luxembourg », ne soit pas alignée sur la pratique générale, à savoir d'archiver les notices JUCHA après trois ans.

Ainsi, pour les affaires d'entraide et de reconnaissance mutuelle, un archivage est en train d'être instauré en pratique. Pour les affaires d'entraide, y compris pour les décisions d'enquête européennes, le délai de base de trois ans sera mis en place et pour les autres instruments européens de reconnaissance mutuelle un délai d'un an sera mis en place. Le délai de trois ans pour les dossiers d'entraide se justifie par la considération qu'il faut assez régulièrement revenir sur des dossiers suite à des demandes d'entraide complémentaires, de sorte qu'un traitement similaire aux dossiers nationaux (l'entraide concerne des crimes et des délits) s'impose. Pour les autres instruments, la procédure s'arrête au moment de l'exécution de la mesure demandée ou peu après, de sorte que l'archivage peut se faire raisonnablement dans un délai plus court. Afin de pouvoir régler les correspondances administratives liées à un tel dossier, un délai d'un an est considéré comme approprié.

Dès lors, il convient d'apprécier la nécessité d'adapter le cadre législatif en matière de coopération internationale afin d'intégrer les délais appliqués en pratique.

Les autres missions des parquets

L'application JUCHA est utilisée aux fins de permettre la restitution d'objets retrouvés parfois longtemps après les faits (p.ex. voitures volées retrouvées à l'étranger, élucidation d'une série de vols ayant permis de retrouver tout ou partie du butin).

L'application JUCHA est en outre utilisée pour « permettre aux procureurs d'Etat d'apprécier la moralité et l'honorabilité d'une personne ». Cette finalité découle de diverses lois sectorielles, notamment de la *loi modifiée du 12 novembre 2002 relative aux activités privées de gardiennage et de surveillance*, en son article 8, et de la *loi modifiée du 7 juin 2012 sur les attachés de justice*, en son article 2, paragraphe 2, point 2. Jusqu'à récemment, ce type d'appréciation a également été effectué sur la base du *statut général des fonctionnaires de l'État* et de la *loi modifiée du 25 mars 2015 déterminant le régime et les indemnités des employés de l'État*.

Or, au vu des disparités des dispositions légales et en l'absence de précision dans lesdites dispositions, on peut s'interroger sur les critères d'appréciation de l'« honorabilité » ou de la « moralité » retenus par le ministère public et de la pertinence de fixer, dans une disposition générale, les données que le ministère public pourra consulter et la période prise en considération pour l'établissement d'une telle appréciation. Il convient de souligner que la législation en vigueur reprend des notions similaires d'« honorabilité » et que l'opportunité de retenir une définition homogène et plus précise de cette notion dans les lois sectorielles précitées pourrait être évaluée, du moins en ce qui concerne les avis demandés aux autorités judiciaires, en énumérant par exemple les traitements de données à caractère personnel auxquels peut accéder le ministère public dans le cadre de l'instruction d'une demande d'avis afin de dégager une pratique cohérente et transparente en cette matière.

Une telle démarche pourrait permettre d'analyser la proportionnalité et la nécessité de la consultation par rapport à la finalité recherchée, en particulier puisqu'il s'agit dans les faits d'une réutilisation de données pour des finalités différentes de celles pour lesquelles elles ont été collectées et eu égard à des questionnements récents relatifs au respect des libertés publiques et de la protection des données personnelles dans ce domaine.

Finalement, comme évoqué plus haut, l'application JUCHA est utilisée pour « garder une trace des dossiers papier transmis aux archives ». A cet égard, étant donné que la majorité des dossiers sont destinés à un archivage définitif auprès des Archives nationales, les notices JUCHA doivent être conservées. Néanmoins, les accès doivent refléter la spécificité de la conservation à des fins d'archivage dans l'intérêt public. Ainsi, tel que la pratique le reflète, seul un nombre très restreint de personnes peut autoriser la consultation de ces notices JUCHA.

D. LES MESURES DE SECURITE

La journalisation et la sécurisation de l'application JUCHA

La loi du 1^{er} août 2018 en matière pénale ainsi qu'en matière de sécurité nationale impose des obligations en matière de sécurité et de protection des données dès la conception et protection des données par défaut, notamment à travers les articles 19 et 28. De même, l'article 24, paragraphe 1, prévoit que

« Des journaux sont établis au moins pour les opérations de traitement suivantes dans des systèmes de traitement automatisé : la collecte, la modification, la consultation, la communication, y compris les transferts, l'interconnexion et l'effacement. Les journaux des opérations de consultation et de communication permettent d'établir le motif, la date et l'heure de celles-ci et l'identification de la personne qui a consulté ou communiqué les données à caractère personnel, ainsi que l'identité des destinataires de ces données à caractère personnel. ».

Les catégories principales d'utilisateurs JUCHA sont les suivantes : le Procureur général d'Etat et les magistrats du Parquet général, les Procureurs d'Etat et les magistrats des parquets, l'inspecteur principal, le juge, le juge d'instruction, le greffier, le secrétaire, le fonctionnaire, l'agent SCAS.

Chaque catégorie principale contient des sous-catégories détaillant la granularité des attributions (voir ci-dessous). Une refonte de ces rôles est actuellement à l'étude.

Le 28 janvier 2020, une nouvelle version de JUCHA (V.4.1.2) a été mise en production qui contient la mise en place technique de la nouvelle interface de gestion des profils d'accès et des permissions dans l'application JUCHA. La version actuelle est la version 4.4, datée du 26 juin 2020. Les releases notes relatives à ces versions ont été fournies à l'ACJ.

Le SIJ est en charge d'organiser les réunions de travail avec les différents services afin de redéfinir les catégories d'accès (casier judiciaire, parquet, cabinet d'instruction, tribunal d'arrondissement de Luxembourg, tribunal d'arrondissement de Diekirch, greffe du tribunal d'arrondissement de Luxembourg, greffe du tribunal d'arrondissement de Diekirch, etc.) et de définir les profils d'accès aux différentes permissions de l'application JUCHA (un total de 345 permissions différentes, qui seront regroupées sous des profils différents, à déterminer dans le cadre des prédites réunions) sous le contrôle des magistrats et du responsable hiérarchique des fonctionnaires/employés du service concerné. Dans le cadre de ces travaux, l'avis des délégués à la protection des données (DPO) respectifs sera également demandé.

Il est prévu de terminer sous peu l'analyse et la refonte des accès pour tous les utilisateurs JUCHA.

Le site intranet de la Justice comporte un formulaire destiné à demander des droits d'accès pour un nouvel utilisateur. Ce formulaire indique, entre autres, l'identité du responsable hiérarchique ainsi que le nom d'une personne de référence travaillant dans le même service que le nouvel utilisateur.

Cette demande est adressée, par la voie hiérarchique, soit, pour le personnel administratif, au bureau du personnel, soit, pour les magistrats, à une personne désignée par le Procureur général d'Etat, en l'espèce un Procureur général d'Etat adjoint, pour validation.

Ce n'est que suite à cette validation que les accès sont mis en place.

En ce qui concerne la journalisation, le comité directeur du projet a validé la liste des événements à tracer lors de la mise en place initiale de l'application de JUCHA. La durée de rétention actuellement en place est de trois ans. Les log-files ne sont accessibles que par le responsable du SIJ, qui procède à une consultation et, le cas échéant, à un export de données en format CSV uniquement :

- sur demande expresse du chef d'administration ou de son délégué en cas de suspicion d'accès illicite (exercice du pouvoir disciplinaire),
- sur demande du DPO en cas de demande émanant d'un tiers ou d'office (RGPD, loi du 1^{er} août 2018 en matière pénale ainsi qu'en matière de sécurité nationale),
- sur réquisition judiciaire (Code de procédure pénale).

Toutefois, le mécanisme de journalisation tel que mis en œuvre actuellement ne permet pas de renseigner avec précision le motif d'une consultation et/ou de modification et nécessiterait éventuellement d'être adapté à l'aune de l'article 24 de la loi du 1^{er} août 2018 en matière pénale ainsi qu'en matière de sécurité nationale.

Les accès aux log-files font également l'objet d'une inscription, y compris d'éventuelles modifications.

Les mesures de sécurité suivantes concernant en particulier l'accès à l'application ont été mises en place :

1. Personnes ayant accès aux données

Les accès sont régis par un système de rôles (techniques) qui déterminent l'étendue des informations auxquelles une personne peut accéder. De manière ponctuelle, le profil individuel d'une personne peut être adapté et inclure des accès supplémentaires, allant au-delà des accès normalement attribués à son « rôle ». Un accès à des informations qui ne sont pas reprises dans le rôle et le profil déterminés est techniquement impossible. Il s'agit donc d'une restriction par onglet d'information. Pour un onglet donné, l'accès n'est pas limité, l'intégralité des dossiers ou des affaires peuvent ainsi être consultés d'un point de vue technique.

- Personnel de l'administration judiciaire

Les demandes d'accès émanant d'un magistrat sont soumises au Procureur général d'Etat adjoint. Les demandes d'un autre membre du personnel de l'administration judiciaire sont soumises au chef du personnel de l'administration judiciaire. Un formulaire spécifique est à utiliser à cette fin. Cette procédure a fait l'objet d'une circulaire d'information et est portée à la connaissance de toute personne concernée au moment où elle demande un tel accès. Le service en charge des statistiques dispose de données issues de l'application JUCHA à des fins de statistiques. L'accès à ces données n'est plus soumis au système de traçage JUCHA.

- Le Service informatique de la Justice

Pour les cas de maintenance ou de résolution de bugs, le personnel du SIJ a un accès de l'application JUCHA en production. Le SIJ et ses prestataires utilisent en partie des données réelles pour tester les applications en cours de développement.

Contrairement aux conclusions retenues par le Parquet général à l'issue de l'analyse d'impact relative à la protection des données (AIPD), le risque d'un accès à des données réelles ou à une copie de ces données, soit par des développeurs, soit par d'autres services, n'est pas suffisamment atténué, les mesures prises ne sont pas suffisantes pour limiter ou contrôler cet accès.

- Prestataires externes

Jusqu'à mars 2020, un seul accès a été accordé à un agent du prestataire externe chargé de la maintenance technique et évolutive de JUCHA. Cet agent a exercé son activité sous la surveillance directe du SIJ. Suite au renforcement du personnel du SIJ en date du 2 décembre 2019, il a été décidé de retirer complètement ce droit d'accès à partir du 1^{er} mars 2020. Depuis cette date, aucun accès n'est accordé à des administrations ou prestataires externes.

2. La revue périodique et la gestion des accès

Une revue des accès est effectuée tous les ans vers octobre, dernièrement en octobre 2019. Cette période a été retenue en raison des nombreux changements qui ont régulièrement lieu à la rentrée judiciaire.

Tout changement d'affectation en cours d'année fait l'objet d'un formulaire spécial qui reprend également les changements requis au niveau des accès. Ce formulaire est nécessaire pour obtenir les droits d'accès requis par la nouvelle fonction, aucune attribution n'a lieu automatiquement par le simple fait de l'affectation.

Un suivi particulier devrait être organisé pour les accès accordés au niveau des profils individuels, étant donné qu'il s'agit d'une exception au principe de l'attribution des accès par rôle.

La gestion des accès, y compris le contrôle des accès, est un processus continu. Actuellement un équivalent temps plein est consacré à la gestion matérielle des accès.

3. Données faisant l'objet de l'accès

En application du principe du « need-to-know », l'accès limité aux informations nécessaires à l'exercice de la tâche incombant au personnel se traduit par le système de rôles qui a été implémenté dans le JUCHA. Le besoin de service est déterminé par les lois applicables, dont notamment le Code pénal et le Code de procédure pénale, ainsi que par la loi sur l'organisation judiciaire. Le concept a été porté à la connaissance des magistrats et fonctionnaires par le biais d'instructions de service. Il a également été porté à la connaissance des agents disposant d'un

accès 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. Ainsi, par exemple, un greffier affecté au cabinet d'instruction a, en raison de son rôle dans l'application, le droit d'accéder à l'onglet « instruction » dans l'application JUCHA sans limites techniques. Cependant, en cas de consultation non justifiée par un besoin de service, l'agent est disciplinairement, voire pénalement, responsable.

4. Authentification et contrôle de l'accès

L'accès est soumis à authentification forte de type « Lux-Trust » et admis uniquement (sauf cas particuliers) à partir d'un poste relié par câble au réseau informatique de l'Etat.

Il n'y a pas de contrôles systématiques, mais les logs sont contrôlés en cas de suspicion d'accès illégitime, par exemple en cas de révélations d'informations secrètes par la presse. Toutefois, comme relevé plus haut, le log ne renseigne pas le motif de la consultation et il appartient à l'agent, en cas de contrôle, d'indiquer ce motif et d'en apporter la preuve en cas de doute.

Il est recommandé de définir des alertes, visant à déclencher une vérification des logs d'accès, en cas d'accès inhabituels, compte tenu de l'ancienneté de l'affaire consultée et du profil d'accès, ou suivant la sensibilité des dossiers consultés.

Il est préconisé de mettre en place une politique de contrôle des logs d'accès visant à revoir ceux-ci de manière périodique et systématique, en particulier pour les notices JUCHA archivées. Une telle vérification périodique des logs constituerait une mesure de mitigation, permettant d'atténuer le risque d'accès non-autorisé par la possibilité de vérifier de manière *ex-post* la justification d'une consultation. Cela accroîtrait le niveau des garanties pour le respect de la vie privée et de la protection des données personnelles des personnes concernées, en prenant en compte la sensibilité des données contenues dans l'application JUCHA, en particulier concernant les notices « archivées », eu égard au droit à l'oubli.

5. Formation et sensibilisation du personnel

Des rappels réguliers par voie d'instructions de service internes relatives à la confidentialité des données inscrites dans JUCHA sont adressés aux agents ayant accès à l'application. Cependant, il convient de noter que les magistrats et les membres de l'Administration judiciaire sont soumis au secret de l'instruction (article 8 du Code de procédure pénale) et à d'autres obligations de confidentialité⁷ dont ils sont censés avoir une parfaite connaissance et pour lesquelles il n'y a pas de rappel régulier général. Le secret des données contenues dans l'application JUCHA, relève, par ailleurs, pour l'essentiel du secret de l'instruction. Des rappels spécifiques ont été envoyés en cas de besoin. Les instructions de service générales relatives à

⁷ Secret des affaires, obligation générale au secret imposée aux fonctionnaires et employés publics.

l'application JUCHA sont transmises au personnel par le Procureur général d'Etat⁸ au même titre que les instructions relatives aux autres traitements internes de la Justice ou bien aux traitements externes auxquels la Justice a accès⁹. Les différentes circulaires sont collectionnées et rendues accessibles en interne à tous les membres de l'Administration judiciaire via un « thésaurus raisonné » disponible sur le site intranet de la Justice. Le dernier rappel, relatif à l'ensemble des traitements de la Justice, remonte au 24 janvier 2019.

Il semble que la pratique mise en place des rôles d'accès et du contrôle des accès convienne, dans l'ensemble, aux exigences en la matière découlant de la loi du 1^{er} août 2018 en matière pénale ainsi qu'en matière de sécurité nationale.

Alors que la journalisation permet d'ores et déjà de retracer convenablement les accès, il est recommandé d'adapter ce mécanisme en prévoyant la saisie obligatoire du motif de consultation et/ou de modification d'une notice JUCHA.

⁸ Le Procureur général d'Etat, en sa qualité de chef d'administration de l'administration judiciaire, envoie en règle générale ces instructions sous la signature du Procureur général d'Etat adjoint en charge de l'informatisation de la Justice.

⁹ Par exemple le registre national des personnes physiques (« RNPP »).

E. CONCLUSION

Nonobstant une gestion de JUCHA ancrée dans des procédures internes, qui, dans l'ensemble, répond aux exigences de la loi du 1^{er} août 2018 en matière pénale ainsi qu'en matière de sécurité nationale et nonobstant le fait que la majorité des traitements de données relatifs aux dossiers papier s'articulent autour des missions principales des juridictions répressives, il apparaît que ni les dispositions du Code de procédure pénale et ni d'autres dispositions légales n'encadrent de manière explicite l'ensemble des caractéristiques des traitements couverts par l'application JUCHA.

Or, si les procédures régissant le fonctionnement de l'application JUCHA semblent adéquates par rapport aux exigences de la législation en matière de protection des données, certains points méritent néanmoins d'être adaptés :

- l'archivage des notices JUCHA devrait être mis en œuvre systématiquement ;
- le mécanisme de journalisation devrait être mis à jour et prévoir que les utilisateurs renseignent avec précision le motif d'une consultation et/ou modification.

Les accès de la société externe qui a développé la gestion de l'application et qui y est impliquée devraient être davantage limités et soumis à un mécanisme de contrôle strict.

Contrairement aux conclusions retenues par le Parquet général à l'issue de l'analyse d'impact relative à la protection des données, le risque d'un accès à des données réelles ou à une copie de ces données, soit par des développeurs, soit par d'autres services, n'est pas suffisamment atténué.

Etant donné que l'application JUCHA regroupe diverses finalités en opérant en fin de compte un rapprochement entre ces différents traitements de données, il pourrait être envisagé d'adopter une disposition générale définissant les éléments essentiels des traitements de données effectués sur base de l'application JUCHA. Une telle démarche pourrait accroître l'accessibilité et la prévisibilité de la loi.

De surcroît, afin que cette démarche permette de tenir compte pleinement des exigences constitutionnelles et conventionnelles découlant de la Convention européenne des droits de l'homme et de la Charte des droits fondamentaux de l'Union européenne et de la jurisprudence telle que citée en début de cet avis, les conditions et modalités desdits traitements devraient être définies dans une base légale spécifiquement dédiée.

Ainsi, il serait recommandé que le législateur adopte une/des disposition(s) spécifique(s) précisant :

- les finalités poursuivies,
- les durées de conservation, les durées d'accès, ainsi que les procédures afférentes,
- les critères d'accès et les procédures afférentes,
- la journalisation et les délais de conservation des logs.

S'il était retenu de légiférer en cette matière, il conviendrait d'adopter des dispositions législatives technologiquement neutres afin de permettre, à terme, d'inclure des traitements de données dans le cadre du projet de la digitalisation des dossiers des juridictions répressives (projet e-Justice).

Luxembourg, le 31 juillet 2020

Le Président de l'Autorité de Contrôle Judiciaire,

Jean-Claude WIWINIUS