Article

Traitement des données par les autorités pénales : de l'accès aux données à la procédure de tri

BENHAMOU, Yaniv, OETTLI, Jean-René

Yaniv Benhamou*/Jean-René Oettli**, Genève

Traitement des données par les autorités pénales : de l'accès aux données à la procédure de tri

Table des matières

I. Introduction

Les autorités pénales sont amenées à traiter régulièrement tous types de données. Les données sont comprises ici comme toute information susceptible d'être utilisée comme moyen de preuve peu importe le support, qu'elle soit consignée sur papier, des supports électroniques (p. ex. disque dur, clef USB, téléphone portable) ou simplement accessibles à distance à travers des appareils personnels[1].

Les autorités pénales doivent par ailleurs traiter un volume croissant de données[2], au risque de ralentir les procédures et de surcharger les autorités de re-

* Professeur associé, avocat, Faculté de droit/Digital Law Center, Université de Genève. Les auteurs remercient vivement Me Emmy Gijs pour son aide efficace à la finalisation de la contribution.

** Avocat, LLM, Genève.

1 ATF 130 II 193, consid. 2.1 ; arrêt du TF 1B_212/2010 du 22. 9. 2010, consid. 4.1.

2 À titre d'exemple, le MPC a dû traiter et trier 19 téraoctets de données saisies entre 2015 et 2018 en lien avec 25 enquêtes liées au football mondial qui, en raison du caractère international, ont conduit à 45 demandes d'entraide judiciaire dans 15 pays, cf. *MPC,* Rapport de gestion 2018, 20.

cours[3]. Au volume des données, s'ajoute le fait que les données sont souvent stockées à l'étranger, ce qui pose des questions d'accès transfrontière aux données. Les autorités pénales cherchent également de plus en plus à saisir les données stockées dans les appareils individuels des personnes arrêtées (p. ex. la procédure opposant le FBI à Apple et visant à accéder au contenu de l'iPhone d'un des auteurs de la fusillade de San Bernardino, M. Syed Farook)[4], voire les données générées par les voitures (p. ex. aux États-Unis, un prévenu est actuellement soupçonné de meurtre en particulier sur la base de l'enregistrement de sa voix extrait de sa voiture par les autorités de police) ou les assistants digitaux (p. ex. l'assistant vocal d'Amazon Alexa ou l'assistant connecté Google Home)[5]. Ces affaires supposent de répondre à différentes questions procédurales : quelles sont les mesures à disposition des autorités pour accéder à ces données, qu'elles soient stockées à l'étranger ou sur les terminaux de personnes arrêtées ? Quels sont les droits et moyens de défense de ces personnes pour s'opposer à de telles mesures ? Dans quelle mesure les autorités pénales doivent-elles tenir compte des principes régissant la protection des données personnelles ?

Répondre à ces questions permet d'apprécier le niveau de protection du droit suisse en matière de protection des données du point de vue des autorités européennes. Celles-ci vérifient en particulier si l'accès aux données et le traitement des données par les autorités étrangères sont conformes aux garanties essentielles européennes afin de déterminer si le pays concerné offre un niveau de protection équivalent à celui de l'Union européenne[6].

3 Cf. arrêt du TF 1B_595/2011 du 21. 3. 2012, consid. 5.3 : le TF s'est déjà reconnu la possibilité de renvoyer l'examen de cas particulièrement importants et complexes à l'autorité de recours. Cf. *Conseil fédéral,* Rapport explicatif concernant la modification du code de procédure pénale, Berne 2017, ch. 2.1.36 : pour désengorger le TF, la modification du Code de procédure pénale (CPP ; RS 312.0) propose de supprimer le délai d'un mois pour statuer sur la requête de levée des scellés et introduire une double instance.

4 Cette procédure a abouti à l'annulation de l'ordre du Tribunal de District (en Californie) de déverrouiller l'iPhone après que le FBI a déverrouillé l'appareil sans l'aide d'Apple, cf. US District Court for the Central District of California CM 16-10 (SP) du 28. 3. 2016, https://assets.documentcloud.org/documents/2778258/2016-03-28-Status-Report-Dckt-209-0.pdf (6. 3. 2021).

5 Cf. *State of New Hampshire v. Timothy Verrill, Docket,* New Hampshire Superior Court No. 219-2017-CR-0072 du 5. 11. 2018, https://www.courts.state.nh.us/caseinfo/pdf/Verrill/110518Verrill-order.pdf (6. 3. 2021).

6 Cf. EDPD, Recommandations 02/2020 sur les garanties essentielles européennes pour les mesures de surveillance, 10 novembre 2020 ; EDPD, Recommandations 01/2020 sur les mesures qui complètent les instruments de transfert destinés à garantir le respect du niveau de protection des données à caractère personnel de l'UE, 10 novembre 2020. Depuis l'arrêt Schrems II, les autorités européennes risquent de renforcer leurs exigences quant à l'analyse de l'accès aux données par les autorités étrangères (appelé parfois *government access*) afin de déterminer si le pays concerné offre un niveau de protection équivalent à celui de l'Union européenne, cf. arrêt CJUE *Data Protection Commissioner c. Facebook Ireland Ltd et Maximilian Schrems* du 16. 7. 2020 (aff. C-311/18).

Dans la présente contribution, nous analyserons d'abord les moyens à disposition des autorités pour accéder aux données (ci-dessous II), en nous concentrant sur les mesures de surveillance rétroactive à l'exclusion de la surveillance en temps réel ou les autres mesures techniques de surveillance prévues à l'art. 280 CPP ou dans la loi fédérale sur le renseignement, avant de nous concentrer sur la procédure de tri par les autorités pénales (ci-dessous III). Nous terminerons par quelques réflexions sur l'interaction entre les règles régissant la procédure pénale et la protection des données (ci-dessous IV).

II. L'accès aux données par les autorités pénales

1. Les différents moyens d'accès aux données

Pour accéder aux données, les autorités disposent de différents moyens. Ceux-ci divergent selon le type de données recherchées (p. ex. tous types de supports et de données ou les données secondaires) et la personne visée par la mesure (p. ex. le détenteur des données ou le prestataire de services).

L'ordre de dépôt (art. 265 CPP)[7] permet à l'autorité d'instruction de demander au détenteur de données de fournir les données requises sans recourir à des mesures de contrainte (art. 265 al. 4 CPP)[8]. La Cour de justice de Genève a récemment assimilé l'ordre de dépôt à des vérifications préalables, soit des mesures qui peuvent être prises par le Ministère public avant l'ouverture d'une instruction formelle[9]. Le

7 Cf. art. 265 al. 2 CPP : ne sont pas soumis à l'obligation de dépôt le prévenu, les personnes qui ont le droit de refuser de déposer ou de témoigner ainsi que les entreprises si le fait d'opérer un dépôt est susceptible de les mettre en cause.

8 ATF 143 IV 21, consid. 3.1 ; arrêt du TF 1B_492/2017 du 25. 4. 2018, consid. 2.1 ; arrêt du TF 6B_247/2017 du 21. 3. 2018, consid. 3.1 ; *Y. Jeanneret/A. Kuhn,* Précis de procédure pénale, 2e éd., Berne 2018, N 14076.

9 CJ GE ACPR/162/2019 du 28. 2. 2019, consid. 2. La question est également traitée de manière incidente dans l'arrêt CJ GE ACPR/519/2018 du 17. 9. 2018, consid. 5 et 5.2. Cf. arrêt du TF 6B_239/2019 du 24. 4. 2019, consid. 2.1 ; arrêt du TF 6B_1096/2018 du 25. 1. 2019, consid. 2.2 ; arrêt du TF 6B_1365/2017 du 27. 6. 2018, consid. 3.3 : les vérifications préalables permettraient ainsi au Ministère public de procéder à certaines vérifications avant de refuser d'entrer en matière (notamment consultation des fichiers, dossiers et renseignements disponibles ou demande d'une prise de position à la personne mise en cause). Cf. également arrêt du TF 6B_431/2013 du 18. 12. 2013, consid. 2.2 ; arrêt du TF 1B_526/2012 du 24. 6. 2013, consid. 2.2 : vérifications préalables avant de refuser d'entrer en matière (art. 309 al. 1 let. a CPP). Cf. toutefois *P. Cornu,* in : Commentaire romand, Code de procédure pénale suisse, Y. Jeanneret/A. Kuhn/C. Perrier Depeursinge (édit.), 2e éd., Bâle 2019, Art. 309 N 3 : la suppression de l'art. 309 AP-CPP (« Investigations préalables ») autorisant le Ministère public à procéder à des vérifications préalables notamment en cas d'infractions complexes priverait désormais le Ministère public de la faculté de procéder à une vérification préalable complémentaire sans l'ouverture d'une instruction formelle.

séquestre (généralement précédé d'une perquisition) permet d'ordonner par voie d'ordonnance au détenteur de données de les remettre (art. 263 CPP). L'ordre de dépôt ou le séquestre couvrent tant les données stockées localement et matérialisées dans un support physique (p. ex. serveurs ou supports de stockage, tels que téléphones portables ou ordinateurs), couvertes par les notions d'« enregistrements » et de « supports informatiques » à l'art. 246 CPP, que les données stockées sur des serveurs distants et accessibles depuis la Suisse[10].

Les mesures de surveillance de la correspondance par poste et télécommunication (art. 269 ss CPP) permettent d'ordonner aux prestataires de remettre certaines données selon des conditions spécifiques[11]. La surveillance rétroactive (art. 273 CPP) porte sur les données secondaires (données d'identification des usagers, de trafic et de facturation), à l'exclusion du contenu des communications possible avec la surveillance en temps réel[12]. Les prestataires visés sont tant les fournisseurs de services postaux et de télécommunication (p. ex. Swisscom) que les fournisseurs dérivés (hébergeurs, fournisseurs d'application tels Google, Facebook et wifi public, tels que les gares et les aéroports) qui ont l'obligation de conserver ces données sur une période de six mois, afin de permettre ces mesures de surveillance rétroactive (art. 273 al. 3 CPP)[13]. Les prestataires visés doivent toutefois se trouver sur le territoire suisse, à défaut de quoi il y a lieu de procéder par la voie de l'entraide internationale en matière pénale[14]. Cette mesure est donc limitée puisque de nombreux fournisseurs de services (en particulier les fournisseurs dérivés) ont leur siège et leur infrastructure à l'étranger.

10 Cf. CR CPP-*Hohl-Chirazi* (n. 9), Art. 246 N 16-17 : la formulation de l'art. 246 CPP est suffisamment large pour appréhender l'arrivée de nouvelles technologies de stockage ou de traitement de données. Cf. *Y. Benhamou,* Blocage de sites web en droit suisse : des injonctions civiles et administratives de blocage au séquestre pénal, in : Droit d'auteur 4.0, J. de Werra (édit.), Genève 2018, 20, relevant que cela repose sur une interprétation extensive du TF qui abandonne la notion « d'objet ou valeurs patrimoniales » au profit de celle « d'accès ou de maîtrise sur les données » et que cette tendance à l'interprétation extensive du texte pour combler certaines lacunes face aux technologies s'observe également dans d'autres décisions. Cf. toutefois *F. Bommer/P. Goldschmid,* in : Basler Kommentar StPO, M. A. Niggli/M. Heer/H. Wiprächtiger (édit.), 2e éd., Bâle 2014, Art. 263 N 27 : approche plus restrictive quant à la notion « d'objet » au sens de l'art. 263 CPP en rappelant qu'il doit s'agir d'objet matériel.

11 Liste d'infractions autorisant le recours à cette mesure (art. 269 al. 2 CPP) et intervention du tribunal des mesures de contrainte (art. 272 al. 1 CPP). Pour une présentation détaillée des différentes mesures de surveillance de la correspondance par poste et télécommunication, cf. *Jeanneret/Kuhn* (n. 8), N 14089 ss ; BSK StPO-*Jean-Richard-dit-Bressel* (n. 10), Art. 263 N 8 ss.

12 Art. 19 al. 4, 21 al. 2 et 22 al. 2 de la loi fédérale sur la surveillance de la correspondance par poste et télécommunication (LSCPT ; RS 780.1).

13 Cf. ATF 139 IV 195, consid. 2.2 ; ATF 139 IV 98, consid. 4.8 : si des données ont été conservées sur une plus longue période, elles peuvent être utilisées et produites dans la procédure.

14 ATF 141 IV 108, consid. 5.3 ; arrêt du TF 1B_142/2016 du 16. 11. 2016, consid. 3.2.

2. L'accès transfrontière aux données stockées à l'étranger

Les moyens évoqués ci-dessus ne sont disponibles que si les données sont stockées en Suisse ou accessibles depuis la Suisse. À défaut, il faudra passer par la voie de l'entraide internationale en matière pénale[15]. Cela pose donc la question de l'accès transfrontière à des données stockées à l'étranger.

En principe, la localisation territoriale des données permet de déterminer la juridiction compétente. Si elles sont localisées en Suisse (i. e. stockage sur des serveurs situés en Suisse), les autorités suisses sont compétentes. Or, les données sont souvent localisées à l'étranger, en particulier lorsqu'elles sont stockées sur des serveurs situés à l'étranger, ce qui suppose de passer en principe par la voie de l'entraide internationale en matière pénale, qu'elle soit ordinaire ou facilitée avec la Convention internationale sur la cybercriminalité (CCC)[16]. De plus, la localisation des données varie souvent constamment, en particulier avec le stockage par l'informatique en nuage public *(Public Cloud computing),* de sorte que l'on peut parler d'une localisation éclatée des données, impossibles à localiser précisément[17].

Pour contourner ces difficultés, la jurisprudence tend à abandonner le critère de la localisation des données (stockage sur les serveurs physiques) au profit du critère de l'accès ou maîtrise sur les données. Par exemple, dans l'arrêt « compte Facebook », il s'agissait d'un cas d'accès direct des données Facebook auprès du prévenu[18]. Le TF a considéré que les données Facebook d'un prévenu accessibles grâce au mot de passe obtenu licitement par les autorités pénales peuvent être séquestrées

15 Cela découle du principe de territorialité du droit international pénal, dont la souveraineté territoriale des États au sens de l'art. 299 al. 1 du Code pénal (CP ; RS 311.0) : il est interdit de violer « la souveraineté territoriale d'un État étranger, notamment en procédant indûment à des actes officiels sur le territoire de cet État ». Le non-respect de ces principes rendrait l'administration des preuves absolument inexploitable (art. 141 CPP). ATF 141 IV 108, consid. 6.2.

16 RS 0.311.43. Pour les États membres de la Convention sur la cybercriminalité, il existe par ailleurs une procédure d'entraide facilitée (art. 22 ss CCC), ainsi qu'une collecte transfrontalière sans passer par la procédure d'entraide judiciaire (art. 32 CCC). Cette collecte transfrontalière est toutefois admissible uniquement si la remise des données est volontaire. Or, le détenteur des données situé à l'étranger requiert souvent une décision judiciaire avant de procéder, de sorte que la remise ne peut être considérée comme volontaire et que l'on retombe sur la voie de l'entraide judiciaire. Pour une analyse de la Convention, cf. *N. Bottinelli,* L'obtention par l'autorité pénale de données informatiques situées à l'étranger, PJA 2016, 1327 ; *D. Rosenthal,* Mit Berufsgeheimnissen in die Cloud : So geht es trotz US CLOUD Act, Jusletter 10. August 2020, qui interprète la Convention à la lumière du US Cloud Act.

17 Cf. PFDPT, Explications concernant l'informatique en nuage (cloud computing), disponible sur https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/Internet_und_Computer/cloud-computing/explications-concernant-l-informatique-en-nuage--cloud-computing.html (6. 3. 2021).

18 ATF 143 IV 270 (compte Facebook), Faits (A).

et que l'importation de ces données Facebook n'est pas un acte accompli « à l'étranger », même si les données sont stockées à l'étranger[19].

Dans les arrêts « Google/Facebook », il s'agissait d'un cas d'accès indirect de données auprès des filiales suisses de Google, respectivement de Facebook[20]. Le TF a admis que la filiale suisse était sujette à un ordre de séquestre, même si les données étaient stockées à l'étranger. Il fallait toutefois qu'elle ait la maîtrise sur les données depuis la Suisse, soit qu'elle ait un pouvoir de disposition effectif sur les données (p. ex. propriétaire ou possesseur des serveurs ou autres supports électroniques sur lesquels les données visées sont stockées)[21] ou un contrôle, soit un pouvoir de disposition en fait et en droit sur ces données (p. ex. l'entité exerçant concrètement des activités de traitement des données et ayant juridiquement l'obligation ou le droit de le faire)[22]. Ainsi, le fait qu'une filiale suisse ait une activité concrète en Suisse n'y change rien si elle n'a pas de pouvoir de disposition en fait et en droit sur les données. En l'espèce, la filiale suisse n'avait pas d'accès ou de maîtrise sur les données, elle ne faisait que de la promotion, la vente, l'affichage d'espaces publicitaires, la vérification de la compatibilité avec les législations nationales et autres activités de représentation de la maison mère[23].

19 ATF 143 IV 270 (compte Facebook), consid. 7.10 (« Celui qui utilise un service internet dérivé, par le biais d'un accès internet à l'intérieur de la Suisse, qui est offert par une entreprise étrangère, n'agit pas ‹ à l'étranger › »). Cette tendance à étendre les prérogatives des autorités pour des données stockées à l'étranger s'observe également à l'étranger. Par exemple, aux États-Unis, le US Cloud Act permet aux autorités américaines de demander aux entreprises sur le sol américain d'accéder aux données sous leur contrôle. En Norvège, une décision de la Cour suprême a admis la perquisition depuis les locaux de TIDAL situés en Norvège, de données stockées sur des serveurs Amazon et Google à l'étranger (TIDAL HR-2019-610-A du 28. 3. 2019).

20 ATF 143 IV 21 (Facebook), consid. 3.4.2 ; arrêt du TF 1B_142/2016 du 16. 11. 2016 (Google), consid. 3.5-3.6.

21 Arrêt du TF 1B_206/2007 du 7. 7. 2008, consid. 2 ; ATF 127 II 151, consid. 4c ; Cf. *Jeanneret/Kuhn* (n. 8), N 14025 : « [a]insi, par exemple, en matière de documentation bancaire, c'est uniquement la banque et non le titulaire ou l'ayant-droit économique du compte qui revêt la qualité de détenteur des informations ».

22 Cf. ATF 143 IV 21 (Facebook), consid. 3.4.2 : « Il apparaît ainsi que la société suisse ne dispose pas d'un accès direct ou d'une quelconque maîtrise sur les données relatives au service ».

23 Cf. ATF 143 IV 21 (Facebook), consid. 3.4.1 : refusant l'analogie avec l'arrêt « Google Street View » (ATF 138 II 346) – qui avait pourtant admis que la filiale suisse avait accès aux données du fait de ses activités de vente d'espaces publicitaires – au motif que cet arrêt concernait une cause de droit public relative à la protection des données qui serait sans rapport avec la question procédurale de détention de données. Cf. *Bottinelli* (n. 16), 1329 : c'est plutôt la nature de l'obligation requise auprès de la filiale suisse qui distingue ces deux affaires : dans l'arrêt « Google Street View », Google est enjointe de ne pas faire (i. e. limiter le type et la nature des données accessibles depuis leur territoire), tandis que dans les arrêts « Google » et « Facebook », elle est enjointe de remettre des données (i. e. rapatrier vers la Suisse et dévoiler des données stockées à l'étranger) avec le risque de violer l'art. 299 CP interdisant la récolte de preuves sur le territoire étranger.

Cette notion d'accès ou de maîtrise sur les données est aussi tirée de l'art. 18 al. 1 let. a CCC, qui exige que les autorités compétentes soient habilitées à ordonner à une personne présente sur son territoire de communiquer les données qui sont « en sa possession ou sous son contrôle ». La condition de données « sous son contrôle » suppose que la personne concernée (ci-après le « contrôleur ») puisse librement y accéder, soit qu'elle ait les capacités techniques et juridiques d'accéder aux données. Les capacités techniques supposent qu'elle puisse avoir accès aux données en clair et faire une recherche de données clients. Les capacités juridiques supposent que le contrôleur ait les autorisations légales nécessaires pour y accéder légalement[24]. Ainsi, dans les groupes d'entreprises, le stockage des données chez une société-sœur ne suffit pas pour considérer que les données sont sous le contrôle de la société-sœur sise en Suisse. Il faudra regarder dans chaque cas d'espèce si l'entité suisse a également l'autorisation légale et technique d'y accéder[25].

Ainsi, pour savoir quels moyens permettront l'obtention de données informatiques, il faut déterminer qui est le contrôleur visé par la mesure (individu ou entreprise sujet à un ordre de dépôt/séquestre, ou prestataire sujet aux mesures de surveillance) et si le contrôleur est localisé en Suisse et a un accès ou la maîtrise sur les données. Sur cette base, on pourra distinguer les quatre moyens d'accès suivants : (i) accès direct aux données (cf. arrêt « compte Facebook »), (ii) accès indirect aux données via le *provider* suisse à la condition que ce dernier ait la maîtrise sur les données et puisse les produire sans engager sa responsabilité (cf. arrêts « Google » et « Facebook »), (iii) accès direct aux données ou accès indirect via le prestataire étranger via la CCC, ou (iv) via les méthodes classiques d'entraide internationale[26].

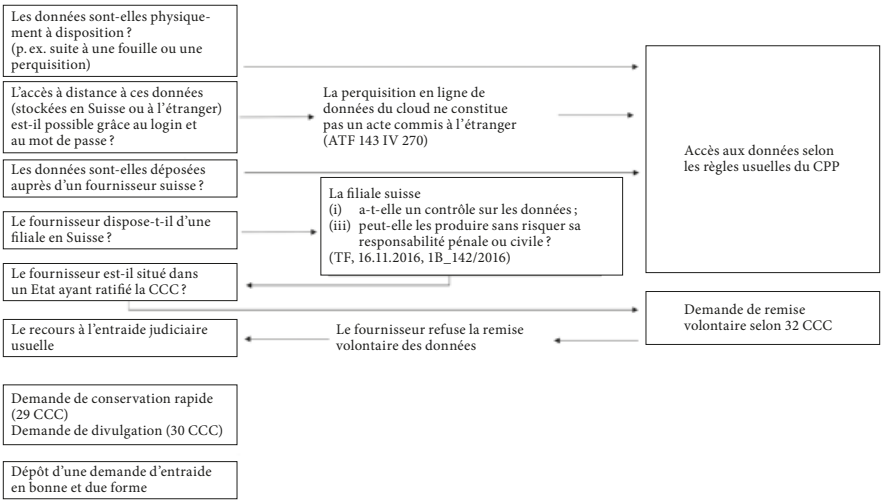
Les différents moyens pour l'accès aux données peuvent être synthétisés comme suit[27] :

24 Il en va ainsi différemment lorsque les données stockées par le prestataire sont cryptées de sorte que lui-même ne peut y accéder. À titre d'exemple, lorsque le compte d'un client de la société ProtonMail est visé par un ordre de dépôt, ProtonMail ne remet pas les correspondances e-mails cryptées mais uniquement certaines métadonnées, à savoir les dates de création et de dernière connexion, à moins que le compte ne soit payant (données d'abonné) ou que l'utilisateur ait activé les logs d'authentification (l'adresse IP associée n'est pas enregistrée par défaut). Cf. notamment https://protonmail.com/blog/transparency-report/ (6. 3. 2021).

25 *Rosenthal* (n. 16), Anhang, N 61 ss.

26 Pour une analyse de l'entraide internationale en matière pénale, cf. *Bottinelli* (n. 16), 1330.

27 Tableau reproduit avec l'aimable autorisation de ses auteurs, *L. Maye/S. Fetter/N. Bottinelli.*



Source : HEG-ARC, CAS pour la magistrature pénale 2019, L. Maye/S. Fetter/N. Bottinelli

On notera enfin que le problème d'accès transfrontière aux données fait l'objet de nombreux débats et propositions horizontales ou sectorielles (p. ex. pour les réseaux sociaux ou certains domaines). À titre d'exemples, une motion du 15 décembre 2016 (Levrat 16.4082) demandait au Conseil fédéral d'imposer aux réseaux sociaux accessibles en Suisse d'y ouvrir une représentation[28] et une motion similaire du 15 mars 2018 (Glättli 18.3306) demandait d'imposer aux grandes plateformes commerciales un domicile de notification[29]. Comme autre exemple, le Conseil fédéral considère actuellement la faisabilité d'un « Swiss Cloud » pour étudier quelles mesures peuvent être prises pour améliorer la souveraineté de la Suisse en matière de données et pour réduire la dépendance des entités suisses aux prestataires internationaux de services en nuage public[30].

28 Motion Levrat 16.4082 du 15. 12. 2016 : Faciliter l'accès des autorités de poursuite pénale aux données des réseaux sociaux, https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20164082 (6. 3. 2021).

29 Motion Glättli 18.3306 du 15. 3. 2018 : Renforcer l'application du droit sur Internet en obligeant les grandes plates-formes commerciales à avoir un domicile de notification, https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183306 (6. 3. 2021).

30 Communiqué de presse du Conseil fédéral du 16. 4. 2020, https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-78814.html (6. 3. 2021).

3. La remise d'une copie des données par le détenteur aux autorités

Pour conclure cette partie, il est intéressant de préciser que le détenteur des données visées par une perquisition ou un séquestre peut conserver ses données ou supports puisqu'il a la faculté de remettre aux autorités pénales une copie des données ou supports informatiques concernés (art. 247 al. 3 CPP)[31]. Une telle copie en lieu et place des supports originaux devrait en règle générale suffire aux besoins de la procédure[32]. Selon nous, les prestataires devraient par ailleurs systématiquement faire usage de cette faculté eu égard à leur devoir de diligence (art. 398 al. 3 CO)[33].

De manière générale, nous estimons que la remise d'une copie devrait l'emporter au nom du principe de proportionnalité[34], en particulier lorsque la mesure est dirigée contre une personne non prévenue (art. 197 al. 2 CPP)[35], sauf lorsque les données sont destinées à un séquestre conservatoire ou en vue de restitution (art. 263 al. 1 CPP), respectivement que leur simple possession soit constitutive d'une infraction (par ex. art. 197 al. 3 CP)[36].

La copie devra consister en une reproduction exacte du support informatique[37]. Lors de la remise d'une copie ou d'une saisie d'un support informatique contenant un système d'exploitation, il conviendra de remettre une image du disque

31 Cf. arrêt du TF 1B_636/2011 du 9. 1. 2012, consid. 2.5.2 : à condition d'exercer cette faculté immédiatement et selon les critères applicables à la requête de mise sous scellés.

32 *N. Schmid/D. Jositsch,* Handbuch des schweizerischen Strafprozessrechts, 3e éd., Zurich/St.-Gall 2017, Art. 247 N 7 ; BSK StPO-*Thormann/Brechbühl* (n. 10), Art. 247 N 28 et 30.

33 RS 220. Cf. ATF 130 IV 43, consid. 1.3 : du devoir de diligence du mandataire (art. 398 CO) et son obligation d'agir dans l'intérêt de son mandant découlent notamment l'obligation de la banque d'avertir immédiatement le titulaire du séquestre de sa relation. Cf. également *Y. Benhamou/L. Tran,* Circulation des biens numériques : de la commercialisation à la portabilité des données, sic ! 2016 571, 584, considérant que, dans le domaine IT, le contrat de mandat constitue la forme la plus classique.

34 CR CPP-*Hohl-Chirazi* (n. 9), Art. 247 N 17 : afin de préserver la bonne marche des affaires, seuls les documents originaux absolument nécessaires seront séquestrés lorsqu'une perquisition a lieu au sein d'une entreprise. BSK StPO-*Thormann/Brechbühl* (n. 10), Art. 247 N 28 : la copie des données sur un support informatique ne saurait intervenir lorsque des tirages papiers de ces documents sont remis à l'autorité. Cf. également *Schmid/Jositsch* (n. 32), Art. 247 N 7.

35 Cf. ATF 141 IV 77, consid. 4.3 : les autorités pénales doivent observer une retenue particulière lors de perquisition de données concernant des personnes non prévenues.

36 BSK StPO-*Thormann/Brechbühl* (n. 10), Art. 247 N 29 et 31 ; *Jeanneret/Kuhn* (n. 8), N 14075.

37 Le Secrétariat de la COMCO se réfère à la notion de sécurisation des données, cf. Secrétariat de la COMCO, Note sur la sélection d'instruments d'enquête, 6. 1. 2016 (« Selon la pratique du Secrétariat, les données électroniques ne sont pas perquisitionnées sur place, mais seulement sécurisées. Cela signifie que le Secrétariat prend connaissance du contenu des données électroniques uniquement dans ses locaux à l'aide d'un logiciel spécifique [forensique]. […] La sécurisation sur place s'effectue soit par le séquestre du support original des données ou par la création d'un duplicata [miroir/image] ou d'une copie »).

permettant l'analyse des données système (log système, log applications, log sécurité, etc.) nécessaire à définir l'accès exercé et l'usage des données examinées[38].

Le refus de l'autorité pénale d'accepter la remise d'une copie des données peut être contesté sous l'angle du principe de la proportionnalité (art. 197 al. 1 let. c CPP)[39], que ce soit dans le cadre d'une procédure d'opposition et de levée des scellés ou par le biais d'un recours si aucune requête de mise sous scellés n'a été formulée[40].

III. La procédure de tri par les autorités pénales

1. La mise sous scellés

Le but de la procédure de mise sous scellés (art. 248 CPP) est d'empêcher l'autorité pénale, en particulier le Ministère public au stade de l'instruction, de prendre connaissance et d'exploiter des informations couvertes par un secret protégé par la loi[41].

Ainsi, lorsque des données entrent en possession de l'autorité, que ce soit à la suite d'une mesure de contrainte (perquisition, séquestre) ou d'un ordre de dépôt[42], leur mise sous scellés peut être immédiatement[43] requise par tout *« ayant*

38 On pensera notamment aux fichiers usrclass.dat sur un système Windows permettant de définir la date de création d'un compte utilisateur, aux fichiers setupapi.dev.log permettant de définir à quelle date un support de données externes a été connecté à un système Windows, aux métadonnées d'un contact Outlook permettant d'identifier le compte e-mail à partir duquel il a été créé, ou à l'historique d'un navigateur internet.

39 ATF 124 I 107, consid. 4c/aa ; CR CPP-*Viredaz/Johner* (n. 9), Art. 197 N 9-10.

40 BSK StPO-*Thormann/Brechbühl* (n. 10), Art. 247 N 32 ; CR CPP-*Sträuli* (n. 9), Art. 393 N 15.

41 *A.V. J. Berthod/G. Megevand,* La procédure de mise sous scellés, RPS 2016 218, 218-219. Par « secret protégé par la loi », on entend un secret applicable à l'ensemble des catégories professionnelles énumérées aux art. 170 à 173 CPP (art. 264 al. 1 CPP). L'art. 248 CPP se réfère également aux enregistrements qui ne sauraient être perquisitionnés ni séquestrés « pour d'autres motifs ». Le Message cite l'exemple d'informations secrètes qui ne sont pas pertinentes pour la procédure (*Conseil fédéral,* Message relatif à l'unification du droit de la procédure pénale, 21 décembre 2005, FF 2006 1057, 1221), ouvrant ainsi la porte à une jurisprudence abondante sur les notions de secret (secret fiscal : arrêt du TF 1B_98/2918 du 29. 5. 2018, consid. 3.4 ; secret d'affaires et commercial : arrêt du TF 1B_447/2015 du 25. 4. 2016, consid. 4.1 ; secret de fabrication : arrêt du TF 1B_98/2918 du 29. 5. 2018, consid. 3.4 ; protection de la sphère privée : arrêt du TF 1B_117/2012 du 26. 3. 2012, consid. 3.3).

42 ATF 144 IV 74, consid. 2.4 ; ATF 143 IV 270 (compte Facebook), consid. 4.6 ; ATF 140 IV 181, consid 2.4.

43 Soit en relation temporelle directe avec la mesure coercitive. Ce délai devrait toutefois être restitué si les conditions de l'art. 94 CPP sont remplies. Cf. arrêt du TF 1B_243/2019 du 19. 12. 2019, consid. 2.4.2 : question de la restitution du délai laissée ouverte dans le cadre d'un recours à la suite de la restitution, par l'instance précédente, d'un délai au Ministère public pour requérir la levée des scellés.

droit », soit toute personne disposant d'un intérêt juridiquement protégé au maintien du secret des données indépendamment de sa maîtrise effective sur ceux-ci[44].

Il appartient d'ailleurs au Ministère public, préalablement à toute perquisition de données, de veiller à ce que le détenteur, soit celui qui les possède effectivement[45], et l'ayant droit aient l'opportunité d'exercer leur droit d'être entendu (en s'exprimant notamment sur leur pertinence pour l'instruction) et demander leur mise sous scellés de manière efficace[46]. Ce devoir d'interpellation est renforcé par le devoir d'information issu des dispositions procédurales de protection des données (art. 95-99 CPP) (ci-dessous IV). En cas de doute, l'autorité pénale doit faire preuve de retenue et procéder à la mise sous scellés de sa propre initiative lorsqu'elle considère que cela est nécessaire à la sauvegarde des droits des personnes concernées[47]. À notre sens, les fournisseurs de services et fournisseurs dérivés sont tenus, tout comme les établissements bancaires[48], de remettre dans les meilleurs délais une copie de l'ordonnance de séquestre non frappée d'une interdiction de communiquer[49] à l'ayant droit afin que celui-ci puisse exercer ses droits (art. 199 CPP)[50].

Saisie d'une demande de mise sous scellés, l'autorité pénale met immédiatement les documents sous scellés et ne peut ni les examiner, ni les exploiter avant l'entrée en force de la décision de levée des scellés prononcée par un tribunal com-

44 Cf. ATF 140 IV 28, consid. 4.3.4.

45 Selon les circonstances, il pourrait s'agir des fournisseurs de services et fournisseurs dérivés qui détiennent les données à titre fiduciaire. Cf. ATF 127 II 151, consid. 4c/aa : en matière de documentation bancaire, c'est uniquement la banque et non le titulaire ou l'ayant droit économique du compte qui revêt la qualité de détenteur des informations.

46 ATF 140 IV 28, consid. 4.3.5.

47 Arrêt du TF 1B_322/2013 du 20. 12. 2013, consid. 2.2.

48 Cf. ATF 130 IV 43, consid. 1.3 ; arrêt du TF 1B_239/2016 du 19. 8. 2016, consid. 3.3 : la banque doit, en vertu des rapports contractuels la liant à son client, notamment l'obligation de diligence découlant de ses devoirs de mandataire (art. 398 al. 2 CO), avertir immédiatement le titulaire de la relation mise sous séquestre, afin que ce dernier puisse se déterminer en temps utile sur la conduite à tenir. Cf. également *C. Lombardini,* Le séquestre pénal d'actifs bancaires : la position de la banque, SJ 2017 II 1, 8.

49 Cf. ATF 131 I 425, consid. 5.1 et 6 : la loi de procédure ne prévoit pas expressément qu'une ordonnance de séquestre peut être assortie d'une interdiction de communiquer. L'interdiction de divulguer la mesure de séquestre est toutefois possible en principe lorsque les besoins liés à la nécessaire confidentialité de l'enquête le justifient. Le principe de proportionnalité doit toutefois être respecté, de sorte qu'une interdiction de communiquer, même si elle s'inscrit dans une enquête complexe, ne saurait être ordonnée durant presque une année.

50 À titre d'exemple, si le compte d'un client d'Infomaniak est visé par une ordonnance de séquestre ou un ordre de dépôt sans interdiction de communiquer, Infomaniak devra, en vertu de son devoir de diligence (art. 398 al. 2 CO), immédiatement aviser son client. A fortiori, dans l'hypothèse où Infomaniak est directement visée par une ordonnance de séquestre ou un ordre de dépôt sans interdiction de communiquer concernant toutes ses données, dont celles de ses clients, elle devrait également les informer de cette mesure.

pétent[51]. Elle ne peut confier les données ou le support physique visé par la requête à la police, même lorsque le mandat à la police porte sur un acte purement technique (p. ex. une copie forensique) et est assorti d'une interdiction de prendre connaissance du contenu[52].

2. La participation au tri judiciaire par le juge des scellés

Il appartient à l'autorité pénale de solliciter la levée des scellés auprès du juge des scellés (art. 248 CPP). C'est dans ce contexte qu'intervient le tri judiciaire des données mises sous scellés qui a principalement pour objet d'écarter de la procédure les données qui ne sauraient être perquisitionnées ou séquestrées. Le juge des scellés évaluera, sur la base des actes d'instruction disponibles, la pertinence des données pour l'instruction selon le critère de « l'utilité potentielle », en écartant celles paraissant manifestement dénuées de pertinence pour l'enquête pénale[53]. Il prendra également les mesures nécessaires afin de préserver, parmi les documents remis aux enquêteurs, la confidentialité des tiers non concernés par l'enquête en cours[54].

Les parties à la procédure de levée des scellés sont l'autorité requérante, le détenteur des données[55] ainsi que toute personne directement touchée dans ses droits (art. 105 al. 2 CPP)[56]. Le prévenu et la partie plaignante ne sont ainsi pas de plein droit parties à la procédure de levée des scellés, à moins de pouvoir se prévaloir d'un intérêt juridiquement protégé au maintien du secret sur certaines données[57].

51 *Berthod/Megevand* (n. 41), 228.

52 Arrêt du TF 1B_443/2018 du 28. 1. 2019, consid. 3.1.

53 ATF 143 IV 462, consid. 2.1 ; ATF 122 II 367 consid. 2(c). Cf. *Berthod/Megevand* (n. 41), 233 : l'application du principe de l'utilité potentielle ne saurait ainsi conduire le juge des scellés à prononcer leur levée du simple fait que les documents pourraient s'avérer pertinents dans une hypothèse vague et lointaine. Cf. arrêt du TF 1B_16/2021 du 31. 3. 2021 : admet l'utilité potentielle des messages, images et videos enregistrés sur un téléphone portable lors d'émentes.

54 ATF 141 IV 77, consid. 4.1 ; ATF 132 IV 63, consid. 4.1 à 4.6.

55 Arrêt du TF 1B_106/2017 du 8. 6. 2017, consid. 2.1 ; arrêt du TF 1B_331/2016 du 23. 11. 2016, consid. 1.3.

56 Cf. arrêt du TF 1B_106/2017 du 8. 6. 2017, consid. 2.1 ; arrêt du TF 1B_288/2012 du 10. 1. 2013, consid. 2.2 : cette notion vise en particulier toute personne qui peut se prévaloir d'un droit de refuser de déposer ou de témoigner et qui pourrait s'opposer à un séquestre en vertu de l'art. 264 CPP. L'atteinte aux droits doit être directe, immédiate et personnelle, une atteinte de fait ou indirecte étant insuffisante.

57 ATF 140 IV 28, consid. 4.3.4-4.3.5 ; arrêt du TF 1B_454/2016 du 24. 1. 2017, consid. 3.2 ; arrêt du TF 1B_331/2016 du 23. 11. 2016, consid. 1.3.

Les parties à la procédure de levée des scellés ne sont pas nécessairement autorisées à participer à la procédure de tri judiciaire, laquelle implique de prendre connaissance du contenu de chacune des pièces sous scellés pour déterminer si elles doivent être restituées à l'ayant droit ou versées au dossier de la procédure[58]. Seul le détenteur des données se voit reconnaître la possibilité de consulter et de se déterminer sur l'ensemble des documents mis sous scellés[59]. La qualité de partie du Ministère public ne l'autorise ainsi pas à participer au tri dont les scellés visent précisément à lui en interdire l'accès[60]. La participation au tri de l'ayant droit et du prévenu non détenteurs ne saurait être plus étendue que ce qui est nécessaire à la sauvegarde de leurs intérêts (art. 105 al. 2 CPP)[61]. À défaut d'un intérêt suffisant pour participer au tri, la partie plaignante devrait pouvoir déduire de son droit de participer à l'administration des preuves (art. 107 al. 1 let. e CPP) la faculté de soumettre des mots-clefs au Ministère public pour qu'il en tienne compte dans ses déterminations à l'intention du juge des scellés[62].

Le droit de participer au tri a pour corollaire une obligation procédurale de l'intéressé d'assister le juge des scellés dans l'examen et le classement des documents, notamment en désignant les pièces qu'il estime couvertes par le secret invoqué ou manifestement dénuées de toute pertinence pour l'enquête pénale[63], ainsi que leur emplacement[64], en particulier lorsque les données mises sous scellés sont

58 CR CPP-*Hohl-Chirazi* (n. 9), Art. 248 N 12d.

59 ATF 142 II 218, consid. 2.3 ; ATF 140 I 285, consid. 6.3.1 ; ATF 135 I 279, consid. 2.3 ; arrêt du TF 1B_346/2013 du 18. 12. 2013, consid. 2 ; *Berthod/Megevand* (n. 41), 236 ; CR CPP-*Hohl-Chirazi* (n. 9), Art. 248 N 12d.

60 Arrêt du TF 1B_345/2014 du 9. 1. 2015, consid. 2.3 ; CR CPP-*Hohl-Chirazi* (n. 9), Art. 248 N 12d. Cf. arrêt du TF 1B_336/2018 du 8. 11. 2018, consid. 4.3-4.4 : le Ministère public doit néanmoins collaborer à la procédure de levée des scellés et fournir des explications circonstanciées sur la pertinence pour son instruction des données en question. Cf. arrêt du TF 1B_637/2012 du 8. 8. 2012, consid. 3.8.1 ; arrêt du TF 1B_200/2007 du 15. 1. 2008, consid. 2.6 : le juge des scellés peut, si nécessaire, interpeller le Ministère public pour obtenir des explications complémentaires s'agissant en particulier de la pertinence des pièces placées sous scellés.

61 Arrêt du TF 1B_264/2013 du 17. 10. 2013, consid. 2.1.2 ; arrêt du TF 1B_539/2012 du 14. 12. 2012, consid. 2.2 ; CR CPP-*Bendani* (n. 9), Art. 105 N 24.

62 CR CPP-*Hohl-Chirazi* (n. 9), Art. 248 N 12f.

63 Arrêt du TF 1B_336/2018 du 8. 11. 2018, consid. 4.3 ; arrêt du TF 1b_63/2017 du 13. 4. 2017, consid. 3.1 ; arrêt du TF 1B_345/2014 du 9. 1. 2015, consid. 2.2. Cf. arrêt du TF 1B_336/2018 du 8. 11. 2018, consid. 4.3 ; arrêt du TF 1B_85/2018 du 3. 7. 2018, consid. 2.1 : les obligations en matière de motivation du détenteur sont d'autant plus importantes que le Ministère public n'a pas accès au contenu des pièces.

64 Arrêt du TF 1B_329/2019 du 14. 10. 2019, consid. 2.4. Cf. également arrêt du TF 1B_602/2020 du 23. 2. 2021 : lors de séquestre de smartphone ou de tablette, il suffit, à défaut de pouvoir accéder aux dossiers concernés, d'identifier les applications (p. ex. e-mail, photos, téléphonie, Threema et/ou WhatsApp) dans lesquelles les fichiers touchant à la sphère privée et intime sont enregistrés, ainsi que les noms des correspondants couverts par le secret professionnel.

très nombreuses ou complexes[65]. Le défaut d'une collaboration suffisante à l'identification précise des pièces entraîne la levée des scellés[66].

Cette obligation procédurale n'emporte pas pour autant celle de remettre à l'autorité le mot de passe, le PIN ou la clef de déchiffrement d'un support informatique ou d'un téléphone portable, ce qui contreviendrait au principe « *nemo tenetur se ipsum accusare* » (art. 158 CPP)[67]. Le juge des scellés ne saurait ainsi sanctionner ce refus de collaborer en refusant d'écarter les pièces protégées par le secret[68] ou contraindre le prévenu à dévoiler ses codes d'accès sous la peine menace de l'art. 292 CP[69], mais devra recourir à l'assistance d'un expert externe ou aux services de police spécialisés (art. 248 al. 4 CPP)[70].

3. La participation au tri non judiciaire par le Ministère public

En l'absence de mise sous scellés ou à la suite de leur levée par le juge des scellés, le Ministère public procède au tri probatoire au cours duquel il revoit libre-

65 ATF 141 IV 77, consid. 4.3 ; ATF 138 IV 225, consid. 7.1.

66 Cf. arrêt du TF 1B_295/2016 du 10. 11. 2016, consid. 3.2.2 : le tri judiciaire, que ce soit par le TMC ou un expert, ne peut être effectué que dans l'hypothèse où l'intéressé aura préalablement indiqué de manière circonstanciée quels documents et/ou données devraient être soustraits de la procédure. Lorsque l'intéressé qui a pu accéder aux données n'établit aucune liste des pièces couvertes par le secret professionnel de l'avocat, l'autorité ne peut pas procéder à la vérification et l'examen de ces pièces et prononcera la levée des scellés. Cf. arrêt du TF 1B_234/2019 ; arrêt du TF 1B_235/2019 du 6. 2. 2020, consid. 4 : dans le cadre de la participation au tri de données issues de surveillance, l'intéressé ne serait se prévaloir de la protection du secret d'affaires et de sa sphère privée pour faire écarter des écoutes téléphoniques alors qu'il n'a (i) ni identifié précisément les pièces à écarter (ii) ni participé au tri des données par le Ministère public nonobstant une invitation formelle à se déterminer.

67 Arrêt du TF 1B_459/2019 du 16. 12. 2019, consid. 2.4-2.5 ; arrêt du TF 1B_376/2019 du 12. 9. 2019, consid. 2.3-2.5. Cf. ATF 143 IV 270 (Compte Facebook), consid. 7.7 et 7.10 : lorsque l'autorité d'instruction apprend (par exemple par une déposition ou une pièce) le code d'accès pour déverrouiller un smartphone saisi (et non scellé) ou un compte Facebook, elle est habilitée à examiner les télécommunications réalisées qui y sont enregistrées (en particulier SMS ou e-mails relevés par le destinataire), y compris les données sur des médias d'enregistrements « clouds » gérés à l'étranger.

68 Arrêt du TF 1B_459/2019 du 16. 12. 2019, consid. 2.5.

69 Cf. arrêt du TF 1B_395/2019 du 10. 10. 2019, consid. 1.3-1.4 : le TF a déclaré irrecevable, faute de préjudice irréparable, un recours d'un prévenu ordonné de remettre les codes d'accès de son iPhone 8 sous la peine menace de l'art. 292 CP, le prévenu étant libre de contester le prononcé d'une éventuelle condamnation dans la procédure au fond.

70 Arrêt du TF 1B_459/2019 du 16. 12. 2019, consid. 2.4-2.5 ; arrêt du TF 1B_376/2019 du 12. 9. 2019, consid. 2.3-2.5. Cf. arrêt du TF 1B_100/2017 du 25. 4. 2017, consid. 2.1 : l'utilité doit s'apprécier sur la base d'indices concrets, étant précisé qu'une utilité potentielle suffit. Cf. arrêt du TF 1B_120/2014 du 20. 6. 2014 : la perquisition à des fins exploratoires (recherche indéterminée de preuves ou « fishing expedition ») est interdite.

ment les données et statue sur la mise sous séquestre de celles utiles à son instruction (art. 263 CPP)[71]. La perquisition, que nous qualifions ici également de tri non judiciaire, intervient ainsi lorsque les données sont lues ou vues par les autorités de l'instruction pour établir leur aptitude à prouver, pour les séquestrer ou pour les verser au dossier[72]. En l'absence de demande de scellés, les données consultées par le Ministère public ne devraient *a priori* pas être de nature à affecter directement les droits que l'art. 248 CPP vise à protéger[73].

La perquisition est limitée aux données dont il *« y a lieu de présumer »* qu'elles contiennent des informations susceptibles d'être séquestrées (art. 246 CPP)[74], à l'exclusion de celles non pertinentes pour la procédure[75] ou protégées par les secrets visés à l'art. 264 al. 1 CPP, que l'autorité compétente doit d'office placer sous scellés sans en prendre connaissance[76]. Le risque d'atteinte aux secrets commerciaux ou privés par le Ministère public est pallié par son secret de fonction[77], étant précisé qu'il lui appartient d'observer une retenue particulière lors de la perquisition de documents concernant des personnes non prévenues (art. 197 al. 2 CPP)[78].

Afin de protéger les intérêts légitimes de confidentialité des tiers[79], le Tribunal fédéral exige que le Ministère public restreigne l'accès au dossier le temps d'effectuer son analyse des données (art. 108 al. 1 let. b CPP), puis prenne les mesures nécessaires à assurer la protection des tiers pour lesquels l'enquête aurait démontré l'absence de lien avec les faits reprochés au prévenu (art. 102 al. 1 CPP)[80]. L'autorité pénale doit ainsi tenir compte de la protection d'autres secrets dont certaines parties à la procédure pourraient tirer profit, ainsi que de la sphère privée du dé-

71 Arrêt du TF 1B_215/2015 du 24. 11. 2015, consid. 4.1.

72 ATF 143 IV 270 (Compte Facebook), consid. 4.4.

73 La perquisition est toutefois propice aux découvertes fortuites pouvant mener à l'extension de l'instruction. Cf. Appellationsgericht BS BES.2019.79, consid. 2 : l'instruction a été étendue suite à la découverte fortuite de pornographie dure lors de la perquisition d'un téléphone portable d'une personne prévenue d'escroquerie par métier.

74 CR CPP-*Hohl-Chirazi* (n. 9), Art. 246 N 3.

75 Cf. arrêt du TF 1B_273/2015 du 21. 1. 2016, consid. 5.1 ; CR CPP-*Julen-Berthod* (n. 9), Art. 263 N 5 : le séquestre probatoire est en effet restreint aux moyens de preuve susceptibles de servir, directement ou indirectement, à la manifestation de la vérité lors du procès pénal, y compris ceux propres à faire la lumière sur la situation personnelle et financière du prévenu (art. 263 al. 1 let. a CPP).

76 CR CPP-*Julen-Berthod* (n. 9), Art. 264 N 1.

77 *Y. Bertossa/J. Droz,* Scellés – mesures de protection ou d'obstruction ?, in : Mélanges à la mémoire de Bernard Corboz, G. Bovey/B. Chappuis/L. Hirsch (édit.), Zurich 2019, 15, N 32, 33 et 36.

78 ATF 141 IV 77, consid. 4.3 ; *Berthod/Megevand* (n. 41), 233.

79 Arrêt du TF 1B_315/2014 du 11. 5. 2015, consid. 4.1.

80 Arrêt du TF 1B_63/2017 du 13. 4. 2017, consid. 3.1 ; arrêt du TF 1B_18/2016 du 19. 4. 2016, consid. 3.4 ; arrêt du TF 1B_439/2012 du 8. 11. 2012, consid. 2.1.

tenteur et des tiers[81]. De telles pièces ne sauraient être versées au dossier que si une mise en balance des intérêts de la poursuite pénale le justifie (par exemple une photo de famille comportant des métadonnées nécessaires à l'instruction)[82] et seront assorties d'une restriction d'accès au dossier[83].

Lors du tri probatoire, le Ministère public verse les pièces utiles à son instruction au dossier sur la base d'une ordonnance de séquestre sujette à recours (art. 263 CPP)[84]. Les pièces écartées par le Ministère public, soit exclusivement celles qui sont manifestement sans pertinence pour l'issue de la procédure[85], ne seront dès lors pas accessibles aux parties à la procédure pénale dans le cadre d'une consultation du dossier. Celles-ci ont néanmoins un intérêt légitime à examiner les données perquisitionnées, serait-ce pour identifier celles potentiellement pertinentes à charge (partie plaignante) ou à décharge (prévenu). Contrairement à une solution retenue par la Cour de justice de Genève, nous estimons que les parties, dans les limites nécessaires à la sauvegarde de leurs intérêts (art. 105 al. 2 CPP)[86], peuvent se voir reconnaître une participation au tri non judiciaire plus étendue que la seule faculté de demander au Ministère public de procéder à toute recherche ciblée justifiée par un intérêt légitime[87].

Le détenteur et l'ayant droit peuvent faire valoir la protection d'un secret ou le manque de pertinence des documents dans le cadre d'un recours contre la perquisition ou la mise en sûreté des supports informatiques[88]. Il serait ainsi contraire au principe de l'économie de la procédure de les empêcher de participer au tri non judiciaire en accédant aux données saisies dans les limites nécessaires à la sauvegarde de leurs intérêts (art. 105 al. 2 CPP), au risque sinon de voir proliférer des demandes de mise sous scellés dans le but détourné[89] d'accéder aux données les

81 *Bertossa/Droz* (n. 77), N 32-35.

82 CR CPP-*Bendani* (n. 9), Art. 108 N. 6.

83 *Bertossa/Droz* (n. 77), N 32.

84 Arrêt du TF 1B_215/2015 du 24. 11. 2015, consid. 5.4 ; ATF 138 IV 153, consid. 3.3.4.

85 Le Ministère public doit verser au dossier toutes les pièces en lien avec l'état de fait (« tatbezogen »). BSK StPO-*Schmutz* (n. 10), Art. 100 N 14 ; *D. Krauss,* Der Umfang der Strafakte, BJM 1983, 62. CJ GE ACPR/604/2018 du 26. 10. 2018, consid. 3.2 ; CJ GE ACPR/88/2012 du 28. 2. 2012, consid. 5.

86 Arrêt du TF 1B_264/2013 du 17. 10. 2013, consid. 2.1.2 ; arrêt du TF 1B_539/2012 du 14. 12. 2012, consid. 2.2 ; CR CPP-*Bendani* (n. 9), Art. 105 N 24.

87 CJ GE ACPR/55/2017 du 7. 2. 2017, consid. 2.4.

88 Arrêt du TF 1B_215/2015 du 24. 11. 2015, consid. 5.4 ; CJ GE ACPR/55/2017, consid. 2.3.

89 Cf. *Bertossa/Droz* (n. 77), N 14-16 : la procédure des scellés a pour but de prémunir les données d'un accès indu par les autorités pénales (art. 248 CPP) et non par les autres parties à la procédure. Selon ces auteurs, lorsqu'un requérant invoque la nécessité de protéger sa sphère privée ou commerciale à l'égard de tiers, la voie des scellés lui est fermée au profit de celles prévues par les art. 264 et 108 CPP.

concernant[90] et de faire écarter celles dépourvues d'utilité potentielle[91]. Le détenteur a par ailleurs la faculté de garder une copie des données lors du séquestre (art. 247 al. 3 CPP). Il serait contraire au principe de proportionnalité à l'exécution de la perquisition (art. 197 al. 1 CPP) de refuser l'accès aux données par le détenteur au motif qu'il a renoncé à en garder une copie lors du séquestre[92].

Refuser l'accès au prévenu en le renvoyant à solliciter des recherches ciblées du Ministère public entraînerait une tension entre son droit de participer à l'administration des preuves à décharge et son droit de ne pas déposer contre lui-même (art. 107 al. 1 let. e ; 113 al. 1 CPP). En effet, si les recherches requises par le Ministère public constituent un « indice d'éventuelle pertinence » pour le juge des scellés[93], celles sollicitées par le prévenu à l'autorité en charge de l'instruction (et non à un juge indépendant) dévoileraient sa stratégie de défense. Il conviendra dès lors d'autoriser la prévenu à accéder aux données saisies tout en prévoyant des aménagements pour assurer que la consultation des données par un prévenu non détenteur des données ne compromette pas les intérêts légitimes de confidentialité des tiers.

La situation des autres parties ne saurait se distinguer de celle qui est la leur devant le juge des scellés. Si elles ne sauraient prétendre à un accès aux données, l'opportunité de participer au tri découle de leur droit de participer à l'administration des preuves (art. 107 al. 1 let. e CPP)[94]. Comme le souligne la cour, il appartient au Ministère public de procéder à toute recherche ciblée par elles requise[95], cas échéant par la soumission d'une liste de mots-clefs.

4. Modalités du tri : indexation et soumission de mots-clefs

Le juge des scellés a la faculté de solliciter l'aide d'un expert pour l'extraction, l'indexation et l'identification des données pertinentes (art. 248 al. 4 CPP)[96]. Les parties peuvent intervenir pour proposer l'expert et définir son mandat, puis pour formuler des observations sur le rapport d'expertise avant que le juge ne rende

90 Arrêt du TF 1B_346/2013 du 18. 12. 2013, consid. 2 ; ATF 140 I 285, consid. 6.3.1 ; ATF 135 I 279, consid. 2.3 ; *Berthod/Megevand* (n. 41), 236.

91 ATF 140 IV 28, consid. 4.3.4 ; arrêt du TF 1B_167/2015 du 30. 6. 2015, consid. 2.1 ; arrêt du TF 1B_206/2014 du 21. 8. 2014, consid. 4.1 ; arrêt du TF 1B_300/2012 du 14. 3. 2013, consid. 3.2.

92 ATF 124 I 107, consid. 4c/aa ; CR CPP-*Viredaz/Johner* (n. 9), Art. 197 N 6-10 ; CR CPP-*Hohl-Chirazi* (n. 9), Art. 247 N 17.

93 Arrêt du TF 1B_336/2018 du 8. 11. 2018, consid. 4.3 ; arrêt du TF 1B_63/2017 du 13. 4. 2017, consid. 3.2.

94 Arrêt du TF 6B_194/2009 du 13. 7. 2009, consid. 2.1.

95 CJ GE ACPR/55/2017 du 7. 2. 2017, consid. 2.4.

96 Arrêt du TF 1B_459/2019 du 16. 12. 2019, consid. 2.4-2.5 ; arrêt du TF 1B_376/2019 du 12. 9. 2019, consid. 2.3-2.5 ; arrêt du TF 1B_19/2013 du 22. 2. 2013, consid. 3 ; *Berthod/Megevand* (n. 41), 234.

sa décision[97]. Selon les circonstances, l'accès au rapport d'expertise peut être restreint à certaines parties (art. 108 CPP), en particulier le Ministère public qui pourrait se voir refuser l'accès au rapport ou se voir adresser une version caviardée afin de protéger le secret des données[98]. Au moment de mandater l'expert, il s'agira pour le magistrat de signaler à son auxiliaire scientifique qu'il attend de lui qu'il respecte les standards de la branche (p. ex. ENFSI)[99].

Dans ce cadre particulier, les tâches déléguées aux brigades spécialisées doivent être limitées à des interventions « purement techniques », en veillant à ce que seule l'autorité judiciaire puisse avoir connaissance des résultats découlant de ces démarches et procède au tri des documents[100]. L'autorité judiciaire doit effectivement s'assurer que les membres de brigades spécialisées ne puissent avoir accès de manière indue au contenu des données protégées par le secret invoqué[101], notamment en raison de l'absence de secret de fonction entre la police, le Ministère public et les tribunaux chargés de la même affaire[102]. Les brigades spécialisées peuvent ainsi être mises en œuvre pour accéder à un support protégé ou des données cryptées[103] ou assister dans la conduite de recherches « aveugles » dont le résultat est ensuite analysé par le juge lui-même[104]. L'installation d'outils permettant le tri de grandes quantités de données peut être déléguée à la police[105], contrairement à la séparation des documents exploitables de ceux dont le contenu est protégé[106].

Lors du tri judiciaire, il est fréquent pour les parties de recourir à une liste de mots-clefs permettant d'écarter une série de données protégées par un secret ou d'identifier et d'extraire celles qui seront pertinentes pour l'enquête[107]. À défaut de

97 Arrêt du TF 1B_345/2014 du 9. 1. 2015, consid. 2.4 ; *Berthod/Megevand* (n. 41), 234.

98 Arrêt du TF 1B_345/2014 du 9. 1. 2015, consid. 2.2-2.3 ; CR CPP-*Hohl-Chirazi* (n. 9), Art. 248 N 15g.

99 *L. Moreillon/J. Vuille/A. Biedermann/C. Champod,* Les nouvelles lignes directrices du European Network of Forensic Sciences Institutes en matière d'évaluation et de communication des résultats d'analyses et d'expertises scientifiques, forumpoenale 2017 105, 109 ss.

100 Arrêt du TF 1B_329/2019 du 14. 10. 2019, consid. 2.2 ; ATF 142 IV 372, consid. 3.1.

101 Arrêt du TF 1B_274/2018 du 27. 1. 2009, consid. 7.

102 ATF 140 IV 177, consid. 3.3.

103 Arrêt du TF 1B_459/2019 du 16. 12. 2019, consid. 2.4-2.5 ; arrêt du TF 1B_376/2019 du 12. 9. 2019, consid. 2.3-2.5.

104 *Berthod/Megevand* (n. 41), 235 ; BSK StPO-*Thormann/Brechbühl* (n. 10), Art. 248 N 39 ; CR CPP-*Hohl-Chirazi* (n. 9), Art. 248 N 15g.

105 ATF 137 IV 189, consid. 5.1.2 ; arrêt du TF 1B_70/2010 du 3. 8. 2010, consid. 6.2 ; arrêt du TF 1B_316/2009 du 8. 3. 2009, consid. 3-4.

106 Arrêt du TF 1B_275/2019 du 12. 8. 2019, consid. 3.3.

107 Arrêt du TF 1B_304/2018 du 13. 11. 2018 ; TPF BE.2017.16 du 25. 5. 2018, consid. 2.8 ; arrêt du TF 1B_63/2017 du 13. 4. 2017, consid. 3.2. Le recours à une liste de mots-clefs est également admissible lors du tri d'informations issues d'une surveillance, cf. CR CPP-*Métille* (n. 9), Art. 271 N 15.

pouvoir participer au tri[108], le Ministère public est appelé à produire une liste de mots-clefs au juge des scellés. Cette liste constitue un « *indice d'éventuelle pertinence* » ainsi qu'une information quant aux objectifs poursuivis par l'autorité pénale[109].

Lors du tri non judiciaire, le Ministère public peut mettre en œuvre un expert privé ou des brigades spécialisées pour l'assister dans l'extraction, l'indexation et le tri de données, ou séparer des autres celles dont le contenu est protégé (art. 247 al. 2 CPP)[110]. Sa tâche pourra en outre consister à examiner le contenu des données, donner son avis quant aux données qui sont pertinentes pour l'enquête pénale ou encore apporter une assistance technique[111]. Le mandat donné à l'expert peut ainsi se limiter à une simple tâche de soutien de l'autorité pénale ou porter sur l'opération de tri elle-même[112].

En l'état, les décisions relatives aux modalités du tri judiciaire (p. ex. le refus de tenir compte de tel ou tel mot-clef soumis par une partie) sont des décisions incidentes qui ne sont pas sujettes à recours au TF, car elles ne sont en principe pas de nature à causer un préjudice irréparable[113]. Ces décisions incidentes doivent en effet être contestées dans un recours contre la décision ultérieure de levée des scellés[114]. Cette situation pourrait cependant évoluer en cas d'adoption d'un double degré de juridiction dans le cadre de la réforme du CPP et la disparition de l'exigence de préjudice irréparable[115]. Dans le cadre du tri non judiciaire, le refus par le Ministère public d'une réquisition de preuve d'une partie tendant à l'utilisation de certains mots-clefs lors de la perquisition ne devrait pas être sujet à recours car une

108 Arrêt du TF 1B_345/2014 du 9.1.2015, consid. 2.3 ; arrêt du TF 1B_336/2018 du 8.11.2018, consid. 4.3-4.4 ; CR CPP-*Hohl-Chirazi* (n. 9), Art. 248 N 12d.

109 Arrêt du TF 1B_336/2018 du 8.11.2018, consid. 4.3 ; arrêt du TF 1B_63/2017 du 13.4.2017, consid. 3.2. Cf. toutefois *Bertossa/Droz* (n. 77), N 57-59 : bien que fréquent dans la procédure de tri, le recours aux mots-clefs n'est pas pour autant la manière la plus efficace d'identifier des pièces utiles à l'instruction, « la consultation d'un élément [étant] susceptible d'influencer immédiatement la recherche du suivant, par l'identification d'une date, d'un intervenant ou par la mention d'un terme auquel l'enquêteur n'aurait pas nécessairement pu penser préalablement ».

110 Pour un exemple, cf. arrêt du TF 6B_398/2019 du 19.7.2019, consid. 6 : cet arrêt souligne d'ailleurs que les frais de la brigade de la criminalité informatique constituent des frais de procédure au sens de l'art. 422 CPP.

111 Arrêt du TF 1B_345/2014 du 9.1.2015, consid. 2.2-2.3 ; CR CPP-*Hohl-Chirazi* (n. 9), Art. 248 N 15g.

112 FF 2006 1057 (n. 41), 1220.

113 Arrêt du TF 1B_63/2014 du 16.4.2014, consid. 1.3 ; arrêt du TF 1B_162/2013 du 3.7.2013, consid. 1.2 ; *Jeanneret/Kuhn* (n. 8), N 651. Pour un contre-exemple, cf. ATF 142 IV 372, Faits (A) : la désignation d'un expert appelé à participer au tri en la personne d'un policier.

114 Arrêt du TF 1B_63/2014 du 16.4.2014, consid. 1.3 ; arrêt du TF 1B_162/2013 du 3.7.2013, consid. 1.2.

115 *Conseil fédéral* (n. 3), ch. 2.1.36.

telle requête peut être réitérée devant le Tribunal de première instance sans causer un préjudice juridique (art. 394 al. b CPP).

IV. La mise en œuvre des principes en matière de protection des données personnelles

1. La protection des données personnelles par les autorités

En présence de données personnelles, l'obtention des données et la procédure de tri par les autorités pénales devront s'effectuer conformément aux dispositions procédurales spécifiques de protection des données (art. 95-99 CPP)[116]. Ces dispositions couvrent tant les données des parties que celles des tiers non-parties à la procédure mais objets directs ou indirects de la collecte (p. ex. données au sujet de personnes contenues dans un support de stockage séquestré dans le cadre de l'enquête de police).

Lorsque les données sont collectées auprès de la personne concernée (p. ex. auprès du prévenu), la collecte doit être proportionnelle et reconnaissable pour la personne[117], sauf si cela peut mettre en péril la procédure[118] ou qu'il n'en résulte un volume de travail disproportionné[119] (art. 95 al. 1 CPP). Lorsque les données sont

116 Ces dispositions ont été adoptées suite à la révision de la loi fédérale sur la protection des données (LPD ; RS 235.1) et la reprise de la Directive (UE) 2016/680 relative à la protection des données en matière pénale. Conseil fédéral, Message concernant la loi fédérale sur la révision totale de la loi fédérale sur la protection des données et la modification d'autres lois fédérales du 15 septembre 2017, FF 2017 6565, 6774 ss. Le traitement des données personnelles dans le cadre de Schengen est en outre régi par la loi sur la protection des données Schengen (LPDS) du 28 septembre 2018 (RS 253.3) qui sera abrogée dès l'entrée en vigueur de la nouvelle loi sur la protection des données (nLPD) (cf. art. 68 nLPD). A défaut de dispositions prévues par la LPDS ou par d'autres lois fédérales spéciales, les dispositions générales de la LPD s'appliquent. La LPDS ne sera pas traitée ici, en particulier vu son champ d'application matériel et temporel limité, et la LPD sera traitée de manière incidente ci-dessous.

117 Le caractère reconnaissable porte sur le principe et l'étendue de la collecte, le type de données et les finalités de traitement.

118 Cette notion doit être interprétée restrictivement mais trouve application, selon nous, lorsqu'une ordonnance de séquestre est assortie d'une interdiction de communiquer pour les besoins liés à la nécessaire confidentialité de l'enquête. L'autorité peut alors ajourner l'information dans les limites du principe de proportionnalité (ATF 131 I 425, consid. 5.1 et 6).

119 Cf. CR CPP-*Fanti* (n. 9), Art. 95 N 28-31 : mentionnant plusieurs exemples de travail disproportionné (p. ex. travail statistique entraînant un volume de travail supplémentaire important s'il avait fallu informer chaque personne concernée par le traitement ou lorsque le fichier comprend de nombreuses données de tiers qu'il convient de caviarder ou d'anonymiser), considérant que ces exceptions supposent une pesée des intérêts et une interprétation restrictive du fait que le devoir d'information est généralement possible sans générer de travail disproportionné.

collectées à l'insu de la personne concernée (p. ex. données de tiers ou du prévenu collectées auprès d'un prestataire), celle-ci doit en être informée sans délai, sauf si un intérêt public ou privé prépondérant exige que l'information ne soit refusée ou ajournée (p. ex. protection de la sphère privée, secrets d'affaires, de témoins ou d'une source) (art. 95 al. 2 CPP). La jurisprudence a développé un « *devoir d'information* » en lien avec la procédure des scellés, lorsque le Ministère public interpelle, avant toute perquisition de données, le détenteur et tout ayant droit afin qu'ils puissent exercer leur droit d'être entendu et cas échéant demander la mise sous scellés[120]. Ce devoir d'information est ainsi renforcé avec ces nouvelles dispositions spécifiques de protection des données (cf. ci-dessus III.1).

Une fois les données collectées, les autorités pénales doivent veiller à traiter les données personnelles en distinguant les différentes catégories de personnes concernées (parties et autres participants au sens des art. 104-105 CPP et personnes reconnues coupables d'infractions et leurs complices ou co auteurs) (art. 95a let. a CPP), ainsi que les données personnelles fondées sur des faits et celles fondées sur des appréciations personnelles (art. 95a let. b CPP)[121]. La distinction entre les catégories de personnes peut évidemment évoluer avec l'avancement de la procédure et il appartiendra à l'autorité compétente de veiller à ne pas porter atteinte à la présomption d'innocence[122]. Elle doit par ailleurs être opérée « *dans la mesure du possible* » de sorte que l'autorité compétente devra s'abstenir de toute qualification lorsque l'état de fait ne permet pas encore de définir la catégorie idoine[123].

La distinction entre les données fondées sur des faits et les appréciations consacre le principe d'exactitude, en vertu duquel les personnes concernées ont un intérêt prépondérant à ce que seules des données actuelles et pertinentes ne soient traitées[124]. Cette exigence de distinction part par ailleurs du constat qu'une procédure pénale est émaillée de « *déclarations contenant des données à caractère personnel* [qui] *sont fondées sur les perceptions subjectives des personnes physiques et ne sont pas toujours vérifiables* »[125]. Il est encore précisé que cette exigence ne doit pas être interprétée de manière trop restrictive[126]. Ainsi, lorsque les autorités pénales

120 ATF 140 IV 28, consid. 4.3.5.

121 Directive (UE) 2016/680 (n. 116), Préambule § 31 ; FF 2017 6565 (n. 116), 6774.

122 Cf. Directive (UE) 2016/680 (n. 116), Préambule § 31 : « Cela ne devrait pas empêcher l'application du droit à la présomption d'innocence ».

123 FF 2017 6565 (n. 116), 6774.

124 CR CPP-*Fanti* (n. 9), Art. 95a N 14 ; FF 2017 6565 (n. 116), 6775.

125 Directive (UE) 2016/680 (n. 116), Préambule § 30.

126 FF 2017 6565 (n. 116), 6774 ; cf. Directive (UE) 2016/680 (n. 116), Préambule § 30 : « [d]ans le cadre des procédures judiciaires notamment, les déclarations contenant des données à caractère personnel sont fondées sur les perceptions subjectives des personnes physiques et ne sont pas toujours vérifiables. Le principe d'exactitude ne devrait par conséquent pas s'appliquer à l'exactitude de la déclaration elle-même mais simplement au fait qu'une déclaration a été faite ».

définissent par exemple le mobile et la personnalité de l'auteur, sa situation personnelle ou l'existence de circonstances atténuantes, elles ne procèdent pas à des appréciations personnelles mais définissent des éléments faisant partie intégrante de la motivation qui n'ont pas à être présentés séparément[127].

À noter enfin l'existence d'un Guide pratique sur l'utilisation de données à caractère personnel dans le secteur de la police[128], lequel s'applique également au travail du Ministère public[129]. Par ailleurs, le procureur général du Canton de Genève a émis des directives au Ministère public et à la police sur le traitement des données signalétiques et des profils d'ADN[130].

2. L'accès aux données personnelles par les parties et les tiers

Il sied enfin de rappeler que les parties, les autres participants à la procédure et les tiers non impliqués dans la procédure peuvent faire valoir certains droits d'accès à leurs propres données personnelles.

Tant que la procédure est pendante, les parties et les autres participants à la procédure ont, dans les limites de leur droit de consulter le dossier, un droit procédural aux renseignements, soit d'obtenir les données qui les concernent (art. 97 CPP)[131]. Ce droit est restreint aux seules parties (art. 104 CPP) et participants à la procédure (art. 105 CPP), à l'exclusion des tiers non impliqués dans la procédure, ceci afin d'éviter d'entraver le bon déroulement de la procédure pénale[132]. Il s'exerce par ailleurs dans les limites du droit de consultation du dossier (art. 101 CPP). En d'autres termes, le droit aux renseignements ne va jamais au-delà du droit de consul-

127 FF 2017 6565 (n. 116), 6775.

128 *Conseil de l'Europe,* Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108), Guide pratique sur l'utilisation de données à caractère personnel dans le secteur de la police du 15. 2. 2018, https://rm.coe.int/t-pd-201-01-guide-pratique-sur-lutilisation-de-donnees-a-caractere-per/16807927d6 (6. 3. 2021).

129 *Procureur général du Canton de Genève,* A.5 Directive sur la gestion et la conservation des données signalétiques et des profils d'ADN, 29 janvier 2015 ; D.5 Directive à la police sur le traitement des données signalétiques et des profils d'ADN, 11. 2. 2015, http://ge.ch/justice/directives-du-procureur-general (6. 3. 2021).

130 *Ibid.*

131 Les termes « données personnelles » et « traitement » à l'art. 97 CPP revêtent la même signification qu'à l'art. 3 let. a et e LPD. FF 2006 1057 (n. 41), 1138. Pour rappel, le droit de consulter le dossier doit être reconnu au plus tard après la première audition du prévenu et l'administration des preuves principales par le Ministère public (art. 101 al. 1 CPP). Outre les parties, les participants à la procédure peuvent exercer ce droit dans la mesure nécessaire à la sauvegarde de leurs intérêts (art. 105 al. 2 CPP).

132 FF 2006 1057 (n. 41), 1138.

ter le dossier[133]. Il est enfin matériellement limité aux données qui concernent la partie à une procédure pendante qui en sollicite l'accès et figurent au dossier, de sorte qu'il ne s'étend pas à toutes les formes de traitement des données dans le cadre d'une procédure pénale ou d'une enquête policière, telles que celles concernant les données de tiers non parties à la procédure[134]. Les tiers non impliqués dans une procédure pendante ne pouvant pas invoquer les droits procéduraux réservés aux parties, ils peuvent se prévaloir du droit d'accès LPD[135] pour accéder à leurs propres données personnelles dans le cadre d'une procédure pendante, en dérogation à l'art. 2 al. 2 let. c LPD[136].

La notion de procédure pendante couvre tout acte effectué par l'autorité pénale ou la police dans le cadre d'une enquête, dont il est parfois difficile de définir le commencement[137], de sorte que tout acte effectué par la police dans le cadre d'une enquête ouvre le droit aux renseignements, étant toutefois rappelé que les parties n'ont en principe pas le droit de consulter le dossier de la procédure pénale durant la phase d'investigation policière autonome[138]. Le mode de communication peut consister en l'autorisation d'une consultation partielle du dossier ou un renseignement écrit fondé sur des questions spécifiques[139]. Un recours peut être formé contre les décisions relatives à une demande de renseignements[140].

Après la clôture de la procédure pénale ou lorsqu'elle est suspendue[141], le droit d'accès aux données est régi par les dispositions cantonales et fédérales sur la protection des données (art. 99 al. 1 CPP). Une procédure est considérée comme étant clôturée au sens de cette disposition lorsqu'elle a abouti à une conclusion juridiquement contraignante[142], soit lorsqu'aucun moyen de droit, même extraordinaire, ne

133 CR CPP-*Fanti/Rohmer* (n. 9), Art. 97 N 20 ; BSK StPO-*Fiolka* (n. 10), Art. 96 N 14.

134 CR CPP-*Fanti/Rohmer* (n. 9), Art. 97 N 1d.

135 Le droit d'accès est actuellement consacré à l'art. 8 LPD. Suite à l'entrée en vigueur de la novelle, le droit d'accès sera consacré à l'art. 25 nLPD, qui détaille les informations à fournir mais reste inchangé dans ses principes. Pour une analyse détaillée du droit d'accès, cf. *Y. Benhamou,* Mise en œuvre judiciaire du droit d'accès LPD : aspects procéduraux choisis, in : Le droit d'accès, S. Métille (édit.), Berne 2021, 77 ss.

136 ATAF A-6356/2016 du 19 avril 2018, consid. 3.1.4 ; ATAF 2016/28 du 30 novembre 2016, consid. 2.2.

137 Cf. CR CPP-*Fanti/Rohmer* (n. 9), Art. 97 N 7 ss : certains auteurs proposent d'examiner au cas par cas le critère du caractère pendant ou non de la procédure.

138 ATF 137 IV 172, consid. 2.3 ; cf. toutefois l'arrêt du Tribunal cantonal vaudois autorisant l'accès au dossier de la police dans le cadre d'une procédure pénale pendante mais sans relation directe avec celle-ci (CDAP VD GE.2011.0034 du 2 mai 2011).

139 FF 2006 1057 (n. 41), 1138.

140 CR CPP-*Fanti/Rohmer* (n. 9), Art. 97 N 3a ; BSK StPO-*Fiolka* (n. 10), Art. 97 N 16

141 TPF BB.2013.75 du 3 juillet 2013, consid. 2.4.

142 ATF 144 IV 81, consid. 2.3.5.

peut être interjeté contre la décision[143]. Cette interprétation permet d'inclure les ordonnances de classement nonobstant le fait que le Ministère public peut, aux conditions de l'art. 323 al. 1 CPP, ordonner la reprise de la procédure préliminaire en tout temps[144]. Selon nous, les données traitées lors de vérifications préalables à une ordonnance de non-entrée en matière devraient pouvoir être obtenues ainsi[145].

L'accès au dossier pénal est dès lors principalement régi par le droit d'accès LPD, étant précisé que la personne concernée ne peut pas consulter l'intégralité du dossier de la procédure close, mais exclusivement ses propres données personnelles, ce qui peut nécessiter des mesures pour préserver les données de tiers (p. ex. anonymisation, caviardage)[146]. La requête est adressée au maître du fichier, soit le Ministère public, qui est considéré dans ce contexte par certaines jurisprudences cantonales comme une autorité administrative de première instance[147]. Il semblerait pragmatique que le Ministère public, saisi d'une requête d'accès, interpelle toutes les parties et, en cas de désaccord entre elles, se réfère au Préposé à la protection des données et à la transparence. En cas d'échec de la médiation, celui rendrait alors une recommandation dont pourrait s'inspirer le Ministère public pour rendre une décision motivée sujette à recours[148].

Une requête d'accès ou de radiation de données inscrites aux dossiers de la police judiciaire est adressée directement au commandant cantonal de la police. La conservation des données personnelles dans les dossiers de la police judiciaire tient à leur utilité potentielle pour la prévention des crimes et délits ou la répression des infractions[149]. Le dossier d'une procédure close est ensuite conservé au moins jusqu'à l'expiration des délais de prescription de l'action pénale et de la peine (art. 103 al. 1 CPP). Même une décision de non-entrée en matière, de classement ou d'acquittement ne suffit pas à exclure que certaines informations concernant la situation de la personne puissent encore apporter des informations utiles, en particulier lorsque les infractions qui ont donné lieu à l'enquête demeurent non élucidées[150]. La radiation de certains documents du dossier de police doit ainsi résulter

143 ATAF A-6356/2016 du 19 avril 2018, consid. 3.1.1 ; ATAF 1-5430/2013 du 28 janvier 2015, consid. 1.3.29 ; ATAF A-4204/2007 du 30 novembre 2007, consid. 4.2.1.

144 ATAF A-6356/2016 du 19 avril 2018, consid. 3.1.3.

145 Cf. arrêt du TF 6B_721/2011 du 12. 11. 2012, consid. 1 : toutes les pièces éditées et réunies par les autorités pénales doivent en effet être versées au dossier dès l'ouverture de l'enquête et à chaque stage de la procédure, y compris durant les investigations policières préliminaires.

146 CR CPP-*Fanti/Rohmer* (n. 9), Art. 97 N 6a.

147 CR CPP-*Fanti/Rohmer* (n. 9), Art. 97 N 11 ; TC FR 601 2018 76 du 13. 9. 2018 ; TC FR 601 2015 110 du 25. 2. 2016 ; OGer ZG GVP 2014, 279, consid. 2.2.

148 CR CPP-*Fanti/Rohmer* (n. 9), Art. 97 N 9.

149 Cf. arrêt CourEDH *Khelili c. Suisse* du 18. 10. 2011 (req. 16188/07), § 59 et 66 : il est notamment proportionnel de conserver au dossier de police judiciaire des données relatives à la vie privée d'une personne condamnée au motif qu'elle pourrait récidiver.

150 ATF 138 I 256, consid. 5.3.

d'une appréciation de toutes les circonstances déterminantes et d'une pesée des intérêts en présence[151]. Ont par exemple été radiées des données qui ne présentaient qu'une faible utilité pour la prévention générale des infractions et qui figuraient toujours au dossier d'une procédure pénale classée[152]. Ont en revanche été maintenues des pièces relatives à des infractions poursuivies d'office, pour lesquelles l'intéressé a été condamné à une amende et ayant trait à son activité professionnelle[153].

V. Conclusion

Pour accéder aux données et les traiter dans le cadre de procédures pénales, les autorités pénales disposent de plusieurs moyens. Elles sont toutefois souvent confrontées à une localisation éclatée des données (p. ex. avec le stockage utilisant les techniques de *Public Cloud Computing*). Une fois les données obtenues, les autorités devront par ailleurs procéder à un tri, tout en respectant en particulier les dispositions en matière de protection des données, la protection des secrets et des intérêts des tiers et des parties à la procédure.

La présente contribution démontre que le cadre légal offre de nombreuses garanties en matière de protection des données, ce qui devrait rassurer les autorités étrangères dans leur appréciation du cadre légal suisse. En particulier, l'accès et le traitement des données par les autorités pénales sont régis par de nombreuses prescriptions confirmées par la jurisprudence, dont le devoir de retenue et d'interpellation du Ministère public en cas de perquisition ou de séquestre des données afin que le détenteur et tout ayant droit puissent exercer leur droit d'être entendu et cas échéant demander la mise sous scellés. De même, les parties peuvent extensivement participer au traitement de leurs données, en particulier dans la procédure de scellés et le tri judiciaire. La présente contribution propose d'apporter des clarifications au cadre légal du tri non judiciaire, lequel doit encore être précisé par la jurisprudence. Enfin, les nouvelles règles procédurales en matière de protection des données viennent compléter et renforcer le droit des parties et des personnes dont les données sont collectées.

151 ATF 138 I 256, consid. 5.5 : la pesée des intérêts en présence tiendra compte de la gravité de l'atteinte portée aux droits fondamentaux du requérant par le maintien des inscriptions litigieuses à son dossier de police, les intérêts des victimes et des tiers à l'élucidation des éléments de fait non encore résolus, le cercle des personnes autorisées à accéder au dossier de police et les intérêts de la police à pouvoir mener à bien les tâches qui lui sont dévolues.

152 Arrêt du TF 1C_307/2015 du 26 novembre 2015, consid. 2. Voir également CJ GE ATA/9/2018 du 9 janvier 2018, consid. 6-8 : accès aux données personnelles figurant dans une main courante.

153 Arrêt du TF 1C_580/2019 du 12 juin 2020, consid. 4.