KONKORDAT NORDWESTSCHWEIZ

Convention intercantonale et inter-autorités relative à l'échange de données pour exploiter des systèmes de suivi et d'analyse de la situation dans le domaine de la délinquance sérielle

Rapport explicatif [Traduction]

1. Origine du projet

1.1. Contexte

Pour lutter efficacement contre la délinquance, il faut pouvoir piloter les ressources policières en fonction de la situation. Les délinquants actuels étant très mobiles, le suivi et l'analyse de la situation requièrent des échanges croissants d'informations entre les cantons. Cela est particulièrement vrai face à la délinquance de masse pratiquée en série. Repérer les délinquants très actifs est un aspect important de la lutte contre ce type de criminalité; il n'est pas moins important de détecter rapidement les séries afin de pouvoir prendre des mesures préventives, même si les auteurs ne sont pas ou pas encore connus. Or, les espaces dans lesquels ces délinquants évoluent dépassent largement les frontières cantonales.

En l'absence de bases légales autorisant le traitement et l'échange entre les cantons de toutes les données utiles concernant la situation dans le domaine de la délinquance, les corps de police ayant adhéré au concordat policier de la Suisse du Nord-Ouest[1], comme leurs homologues de la plupart des autres concordats, sont limités à leur territoire cantonal pour monitorer et analyser la délinquance sérielle. Ils ne peuvent donc établir qu'un tableau incomplet de la situation. Les partenaires concordataires échangent leurs renseignements par des voies conventionnelles[2], qui sont lentes, inefficaces, incomplètes, gourmandes en ressources et d'une technologie obsolète.

Il est actuellement impossible de procéder à une analyse approfondie visant à détecter les délinquants très actifs et les séries d'infractions pour avoir une base sur laquelle appuyer une lutte efficace. Il faudrait que les partenaires concordataires disposent d'outils d'analyse communs permettant les échanges de données par une procédure d'accès en ligne. Il est important d'automatiser le plus possible les étapes de travail afin que les services de suivi et

[1] Concordat du 20 janvier 1995 réglant la coopération entre les polices de la Suisse du Nord-Ouest.
[2] Rapport hebdomadaire au centre régional de suivi de la situation et échanges de renseignements sur des cas individuels par courrier électronique ou téléphone.

d'analyse de la situation de la police soient déchargés et puissent consacrer davantage de temps au travail d'analyse proprement dit.

Il est important de pouvoir présenter les faits mis au jour sous des formes adaptées aux différents destinataires (rapports, cartes interactives, représentation graphique des liens entre les éléments personnels et les éléments matériels, etc.), que ce soit pour servir de base de décision objective en vue de planifier des mesures, pour faire avancer des enquêtes ou pour rédiger des notes d'information et des recommandations concrètes.

De tels outils d'analyse sont déjà utilisés dans certains cantons, avec grand succès d'ailleurs. Mais pour en exploiter tout le potentiel, il faut que ces banques de données soient constituées et exploitées à l'échelle intercantonale. C'est le seul moyen pour réussir à dresser un tableau complet de la situation en matière de délinquance sérielle transcantonale et mettre en évidence des tendances et des liens qui seraient sinon impossibles à établir. Il faut en outre que les renseignements actuellement fournis par des tiers à chaque canton séparément pour alimenter l'analyse (p. ex. les «signalements nationaux» émanant d'autres corps de police) ne soient saisis qu'une seule fois afin, là encore, de dégager davantage de temps pour l'activité d'analyse proprement dite.

Il n'existe pas encore de banques de données communes permettant de travailler sur des espaces de délinquance intercantonaux. Or, cette approche est nécessaire pour établir des pronostics concernant les espaces vulnérables à la délinquance à l'échelle régionale. Elle permettrait de coordonner la gestion des points critiques d'importance régionale, ce qui aurait indubitablement un impact positif sur les ressources.

1.2. Outils

Le développement d'applications de police s'est multiplié ces dernières années et il y a tout lieu de croire que cette évolution se poursuivra. C'est pourquoi la présente convention, plutôt que de se limiter à une application déterminée, est rédigée de façon à permettre l'utilisation de plusieurs applications, existantes ou à venir. Ainsi, le risque que la base légale soit en permanence en retard sur les progrès techniques diminue. En revanche, pour respecter la législation sur la protection des données, les renseignements dont la saisie est autorisée sont désignés avec précision. À dessein, la convention ne détaille pas la nature des interconnexions ni le fonctionnement des applications, qui seront régis dans les règlements d'exploitation.

Les deux outils d'analyse présentés ci-après ont connu une très large diffusion ces dernières années.

1.2.1. PICAR[3]

Le système PICAR est utilisé depuis 2008 comme plateforme d'analyse commune par les membres du CICOP[4]. Cette banque de données d'incidents offre un outil d'analyse de la délinquance sérielle axé sur les infractions contre le patrimoine (vols avec effraction, dans les commerces, par astuce, etc.), la violence et les délits à caractère sexuel. Les séries et les tendances peuvent être détectées rapidement et systématiquement grâce à la centralisation de la saisie et de l'analyse des cas et des relations entre les cas[5]. La plateforme permet notamment de réaliser des représentations et des évaluations rapides de la délinquance sérielle, des rapprochements entre des séries identifiées ou encore des comparaisons entre des photos d'auteurs inconnus.

Le système PICAR est adapté en permanence au plus près des besoins des corps de police qui en sont membres grâce au travail d'administration et de développement fourni à l'interne[6].

Dans le concordat policier de la Suisse du Nord-Ouest, la police de Bâle-Campagne et la police cantonale d'Argovie utilisent PICAR depuis 2014 et 2015 dans des banques de données cantonales séparées. Ces banques de données, qui sont accessibles à tous les policiers et policières du canton, sont alimentées par des informations provenant d'autres systèmes de police (p. ex. Journal, ABI, Vulpus). Mais seul le regroupement de ces renseignements dans une banque de données commune permettra d'avoir une image de la situation valable pour les deux cantons.

1.2.2. PRECOBS

PRECOBS[7] est un logiciel de prévision par modélisation développé par l'*Institut für musterbasierte Prognosetechnik* d'Oberhausen[8], en Allemagne.

PRECOBS travaille sur la base du phénomène de répétition proche (*near repeat phenomenon*)[9]. Un algorithme analyse des données policières telles que les lieux où des délits ont été commis, les modes opératoires, les outils utilisés, les objets dérobés et d'autres éléments empiriques réunis dans des affaires passées pour identifier des concentrations spatiales et temporelles. Sachant que la probabilité que ces concentrations se répètent est

[3] Plateforme d'Information du CICOP pour l'Analyse et le Renseignement.
[4] Concept Intercantonal de Coordination Opérationnelle et Préventive (concordat réglant la coopération en matière de police dans les cantons romands et au Tessin).
[5] Relations reposant sur des éléments situationnels et des traces matérielles. Ce sont uniquement les liens, et non pas les éléments et les traces, qui sont enregistrés.
[6] En règle générale par des collaborateurs et collaboratrices ayant une formation scientifique (master de l'Université de Lausanne).
[7] Pre Crime Observation System.
[8] IfmPt; cf. https://www.ifmpt.de/.
[9] Lire p. ex. GLUBA, ALEXANDER: *Predictive Policing – eine Bestandsaufnahme. Historie, theoretische Grundlagen, Anwendungsgebiete und Wirkung* – Hanovre: LKA Niedersachsen, 2014, p. 3.

très élevée, le logiciel définit alors des zones vulnérables. Si un délit est commis dans l'une de ces zones, la probabilité que d'autres délits y soient perpétrés dans les sept jours augmente. La police peut ainsi mettre en place des mesures de prévention et de répression ciblées tout en utilisant ses ressources de façon économe.

C'est la police de la ville de Zurich qui a été la première police à mettre en place le logiciel PRECOBS en 2014. Elle a été suivie par la police de Bâle-Campagne fin 2014 puis par la police cantonale d'Argovie.

2. Démarche

2.1. Mandat

L'autorité du concordat policier de la Suisse du Nord-Ouest a décidé, le 9 décembre 2016, d'instituer un groupe de travail des cantons concordataires placé sous la direction de la police de Bâle-Campagne. Le groupe de travail a été chargé d'examiner, avec le concours de la Conférence des préposé(e)s suisses à la protection des données, s'il était possible d'étendre le concordat afin que les cantons puissent exploiter conjointement des systèmes de conduite d'interventions et des logiciels de suivi et d'analyse de la situation et échanger automatiquement les renseignements requis à cet effet. Il fallait déterminer en particulier dans quelle mesure il était nécessaire d'apporter des adaptations au concordat ou à la loi sur la police des cantons concordataires, voire aux deux.

2.2. Groupe de travail

Le groupe de travail se composait de représentantes et de représentants des services de la protection des données des cantons d'Argovie (pas en permanence), Bâle-Ville, Bâle-Campagne, Berne et Soleure, des services juridiques des polices cantonales de Bâle-Ville, Berne et Soleure, d'un utilisateur de PICAR (police cantonale d'Argovie) et des chefs de la police judiciaire des cantons de Bâle-Ville et Bâle-Campagne.

2.3. Rapports intermédiaires et décisions

Lors de sa réunion du 9 juin 2017, l'autorité concordataire a renoncé à étendre le concordat existant en s'appuyant sur une base légale à inscrire dans les différentes lois cantonales sur la police pour exploiter des systèmes intercantonaux de suivi et d'analyse de la situation. Elle a préféré élaborer une base légale revêtant la forme d'une nouvelle convention intercantonale autonome. Cette convention serait dans un premier temps conclue par les cantons de la Suisse du Nord-Ouest, mais elle serait ouverte aux autres cantons. Il faudrait également obtenir l'adhésion du Corps des gardes-frontière (CGFR), qui est aujourd'hui déjà un important fournisseur de renseignements.

2.4. Consultation

Les gouvernements des cantons parties au concordat policier de la Suisse du Nord-Ouest ont été invités à prendre position sur le projet de convention par courrier du 18 décembre 2018. Tous les gouvernements ont répondu. Les propositions de modification ont pu être prises en compte en grande partie; lorsque cela n'a pas été le cas, il en est fait mention dans le présent rapport.

3. Contenu, conception et structure de la convention

3.1. Principe

Dans le cadre de la présente convention intercantonale, les parties exploitent des systèmes de suivi et d'analyse de la situation susceptibles de contenir des données personnelles sensibles (art. 8). Cela requiert une décision du pouvoir législatif compétent.

La convention indique les organes nécessaires à l'accomplissement des tâches prévues et elle en définit la composition et les tâches. Elle décrit en outre dans leurs grandes lignes les principes régissant tous les logiciels, les conséquences financières de la sortie d'une banque de données commune et les rapports de responsabilité mutuelle entre les parties.

La convention définit notamment:

- le but des banques de données et du traitement des données,
- le contenu des banques de données et les catégories de données,
- les règles d'échange de données,
- les droits d'accès,
- les délais de conservation, l'archivage et l'effacement des données,
- le droit d'information et la protection juridique,
- les principes de base de l'organisation,
- les principes de base du financement.

Elle crée la base légale nécessaire pour exploiter légalement, dans le respect du principe de proportionnalité, différents systèmes intercantonaux de suivi et d'analyse de la situation. Il est actuellement surtout question des logiciels PICAR et PRECOBS. Il est cependant envisageable, vu l'évolution des technologies, que de nouvelles applications ayant le même but mais des architectures différentes arrivent sur le marché. La convention a donc été, à dessein, formulée de manière à pouvoir constituer une base légale pour l'utilisation de futurs nouveaux produits tout en restant en conformité avec son objet.

3.2. Structure à deux niveaux

La convention ayant pour but de créer une base légale pour l'échange de données qui soit conforme au droit et claire, sans empiéter sur les compétences des législateurs cantonaux, le choix a été fait de lui donner une structure à deux niveaux.

3.2.1 Niveau stratégique: adhésion à la convention

Le fait d'adhérer à la convention n'oblige pas les parties à exploiter ensemble l'une ou l'autre application. Le canton ou le service fédéral qui adhère à la convention devient simplement partie à la convention, ce qui lui donne la possibilité de participer ou non à l'exploitation commune d'une ou plusieurs banques de données (cf. art. 2, al. 1, phr. 2). L'autorité compétente fait un choix pour chaque banque de données individuellement, en fonction de ses besoins et de l'utilité qu'elle en attend.

3.2.2 Niveau opérationnel: participation aux banques de données

Différentes banques de données pourront être exploitées dans le cadre de la présente convention, par un ensemble de participants variable selon les cas.

Un canton ou un service fédéral qui est partie à la convention acquiert le statut de participant à une banque de données après en avoir approuvé le règlement d'exploitation[10]. Le règlement d'exploitation d'une banque de données définit avec précision les modalités de son exploitation ainsi que les droits et les devoirs de ses participants. Ces règles peuvent varier d'une application à l'autre. Les cantons et les services fédéraux décident ainsi en toute connaissance de cause de participer à telle ou telle banque de données.

Chaque banque de données sera soumise au contrôle préalable du service de protection des données compétent, auquel devront être présentés à cette fin le règlement d'exploitation et un concept de sûreté et de protection de l'information (SIPD).

Dans le cas de PICAR, les travaux de projet sont déjà bien avancés. La police de Bâle-Campagne a été pressentie pour faire office de service central[11] tandis que la police cantonale d'Argovie se prépare à assumer la fonction de service extérieur. D'autres polices cantonales ont signalé leur intention d'adhérer à la convention dès que cette base légale sera en vigueur.

3.3. Organes

La mise en œuvre de la convention requiert une certaine organisation (cf. art. 3 à 5)[12].

---

[10] La convention et le rapport explicatif font systématiquement la distinction entre les parties à la convention et les participants aux banques de données. Les cantons et les services fédéraux qui adhèrent à la convention ne prennent pas d'engagement, mais s'assurent simplement la possibilité de participer ultérieurement à une ou plusieurs banques de données communes dans le but et conformément aux principes énoncés dans la convention: ce sont les parties à la convention. Lorsque les parties à la convention font usage de cette possibilité, elles deviennent des participants à telle ou telle banque de données.

[11] Cf. ch. 3.3.3.

[12] Les réponses à la consultation ont montré des divergences entre les cantons sur ce point: plusieurs auraient préféré une organisation plus simple, mais pour d'autres l'absence d'organe de surveillance aurait été rédhibitoire. L'organisation choisie répond ainsi au souhait de permettre à tous les cantons d'adhérer à la convention.

3.3.1. Organe de surveillance intercantonal

Un organe de surveillance intercantonal veille à la bonne application de la convention (cf. art. 3). C'est également à lui qu'il incombera de présenter les rapports périodiques exigés par la législation de différents cantons lorsque des conventions de cette nature sont conclues.

L'organe de surveillance se compose de représentantes et de représentants des gouvernements cantonaux et des responsables politiques des services fédéraux parties à la convention. Ces personnes sont nommées en application du droit cantonal pour les premières et du droit fédéral pour les secondes.

3.3.2. Comité directeur

Un comité directeur assure la direction et la mise en œuvre stratégiques de la convention ainsi que le règlement des différends (cf. art. 4). Son activité est limitée à des actes de gestion[13].

Le comité directeur se constituera lui-même, mais il serait logique que ses membres représentent le niveau hiérarchique des commandantes et commandants de police et des cheffes et chefs de police judiciaire ou de division de police judiciaire.

3.3.3. Service central et services extérieurs

La direction opérationnelle de chaque banque de données sera assurée par un service central, avec le concours de services extérieurs (cf. art. 5). La convention définit des principes d'organisation généraux qui s'appliquent de la même manière à toutes les banques de données. Les détails techniques, organisationnels et financiers et les modes de fonctionnement seront établis dans un règlement d'exploitation pour chaque banque de données, toujours en restant dans le cadre de la présente convention.

Pour des raisons de ressources, il n'est pas raisonnable de penser qu'un seul corps de police puisse et veuille assumer la responsabilité opérationnelle de toutes les banques de données en endossant la fonction de service central.

3.4. Droit supérieur

Les logiciels de suivi et d'analyse de la situation utilisent entre autres des données recueillies en application du CPP[14].

Selon l'article 2, alinéa 2, lettre *c* LPD[15], les procédures pénales pendantes sont exclues du champ d'application du droit général de la protection des données. Le CPP contient ses

[13] Il est exclu que le comité directeur édicte des dispositions fixant des règles de droit. Si l'exploitation d'un logiciel actuel ou futur nécessitait des dispositions de cette nature, il faudrait compléter la convention par la voie législative ordinaire.
[14] Code de procédure pénale suisse du 5 octobre 2007, Code de procédure pénale, CPP; RS 312.0.
[15] Loi fédérale du 19 juin 1991 sur la protection des données (LPD; RS 235.1).

propres principes applicables au traitement des données (art. 96 à 99). L'article 96, alinéa 1 CPP, par exemple, autorise expressément à établir des interconnexions systématiques entre des cas différents[16]. Les articles 95 à 99 constituent ainsi des règles de droit spécial qui s'appliquent tant qu'une procédure pénale est pendante au sens strict. Leur champ d'application ne s'étend donc pas aux renseignements qui, après avoir été recueillis dans le cadre d'une procédure pénale, seraient conservés dans une banque de données jusqu'à leur effacement conformément à la loi. Dans ce deuxième contexte, ce sont en principe les règles générales de la Confédération et des cantons en matière de protection des données qui s'appliquent[17].

4. Commentaire des dispositions

Titre

La présente convention ne porte pas le titre de concordat car les concordats sont généralement conclus entre cantons alors que la présente convention est ouverte aux «services appropriés de la Confédération» (art. 17)[18], tel le Corps des gardes-frontière, qui est un important fournisseur de renseignements. Pour la même raison, la convention est qualifiée d'intercantonale et inter-autorités, et non pas d'intercantonale seulement[19].

Préambule

Le préambule fait référence à l'article 56 de la Constitution fédérale de la Confédération suisse du 18 avril 1999 (Cst.)[20] car il est envisageable, même si ce n'est pas prévu actuellement, que la Police nationale ou la gendarmerie françaises, la police fédérale allemande ou la police du Land de Bade-Wurtemberg adhèrent à la convention[21]. La lutte contre la criminalité transfrontalière donne lieu à des échanges d'informations nourris avec ces organisations dans le cadre traditionnel. Mais comme la convention, dans sa version actuelle, est ouverte uniquement aux cantons et aux services fédéraux appropriés[22], il faudra d'abord l'adapter par la voie législative ordinaire. En l'état, ces autorités étrangères peuvent fonctionner seulement comme fournisseurs indirects de renseignements et il n'est pas possible de les autoriser à accéder aux banques de données[23].

---

[16] NIGGLI, MARCEL ALEXANDER / HERR MARIANNE / WIPRÄCHTIGER HANS (éd.): Schweizerische Strafprozessordnung / Jugendstrafprozessordnung, 2e éd., Bâle 2014, ci-après «BSK-StPO», GERHARD FIOLKA, art. 96 no 1.
[17] BSK-StPO-GERHARD FIOLKA, op. cit., remarques liminaires ad art. 95-99 no 3.
[18] Voir aussi le commentaire de l'art. 17.
[19] Cf. titre, préambule et art. 1, al. 1.
[20] RS 101.
[21] Voir aussi le commentaire de l'art. 19.
[22] Art. 17, al. 1.
[23] P. ex. les autorités policières communales dont les informations alimentent les banques de données via les polices cantonales.

Article 1

La mission la plus importante de la police consiste à prévenir les infractions, raison pour laquelle il faut détecter les séries et y mettre fin dans les meilleurs délais. De plus, les informations et les éléments ainsi recueillis contribuent à identifier les auteurs et à les traduire en justice.

Les délits en série sont des délits commis de manière répétée ou par les mêmes auteurs. Mais une série commence forcément par un premier acte délictueux. Il faut donc pouvoir l'enregistrer, en particulier s'il s'agit d'un méfait typiquement commis en série et donc susceptible de marquer le début d'une série.

Il n'existe pas de définition scientifique de la délinquance sérielle. Dans la pratique, les séries les plus importantes en nombre sont observées dans la catégorie des infractions contre le patrimoine (vols par effraction, par introduction clandestine et par ruse, vols à l'arraché, vols de sacs, vols dans les magasins, effraction d'automates, fausse monnaie, vols de véhicules et dans les véhicules, vols de plaques minéralogiques, utilisation abusive d'installations de traitement de données, agressions à main armée, dommages à la propriété, incendies et explosions). Mais les délits sexuels (commis sur des personnes n'appartenant pas à la famille ou à l'entourage connu) et les délits de violence (p. ex. homicides) donnent eux aussi lieu à des séries. En revanche, on ne compte pas dans les délits en série les infractions à la législation sur les stupéfiants et les délits sexuels commis contre des personnes dans la famille ou l'entourage.

Sans définir la délinquance sérielle, le titre et l'article 1, alinéas 1 et 2, précisent que le champ d'application de la convention est limité à ce type de délinquance.

Les banques de données du type de celles visées par la convention contiennent à la fois des données validées et des données non validées. Les tableaux de situation contiennent typiquement une proportion variable d'informations non validées, qui ne sont donc pas encore propres à être exploitées dans une procédure pénale. Il est usuel d'avoir connaissance au cours d'une procédure pénale d'éléments qui donnent une vraisemblance accrue à des données non validées ou qui les corroborent. Les données en question sont ainsi validées, ce qui permet de les exploiter éventuellement en application du CPP. Inversement, il peut apparaître au cours d'une procédure que des informations non validées sont fausses. Ces constats intervenus a posteriori ne rendent pas illicite le traitement des données effectué antérieurement, mais ils peuvent entraîner une rectification ou une suppression des données en question[24].

[24] Cf. art. 12 et 13.

Article 2

L'article 2 établit la structure à deux niveaux[25] qui permet à la convention de constituer une base légale ouverte sur l'avenir pour l'échange de données et la coopération entre les parties. Plutôt que de fixer des règles pour des banques de données déterminées, cette disposition instaure un cadre pouvant s'appliquer à une grande variété de banques de données et de participants. Cela permet d'adhérer à la convention sans devoir automatiquement participer à toutes les banques de données. La structure se compose d'un niveau supérieur (la convention), qui définit les fondements des échanges, et d'un niveau inférieur (les règlements d'exploitation), qui régit les modalités concrètes d'exploitation des banques de données.

L'article 2, alinéa 1 est central car il confère un caractère obligatoire à la structure à deux niveaux que nous venons de décrire tout en expliquant son fonctionnement. La formulation «un règlement d'exploitation est établi pour chaque banque de données commune» signifie qu'il est possible d'exploiter de multiples banques de données au titre de la présente convention, d'une part, et que chacune de ces banques de données doit être dotée d'un règlement d'exploitation conforme aux règles supérieures fixées dans la convention, d'autre part. Concrètement, les règlements d'exploitation doivent définir de manière exhaustive et expresse tous les aspects techniques, organisationnels et financiers.

L'article 2, alinéa 1, phrase 2 précise que l'adhésion à la convention n'entraîne pas automatiquement l'adhésion à l'ensemble des banques de données exploitées au titre de la convention et que les parties ont la possibilité de participer seulement aux banques de données qui les intéressent.

Article 3

La législation de plusieurs cantons oblige à prévoir un organe chargé de surveiller le respect de la convention. Il faut donc que le comité directeur (cf. art. 4) soit tenu de rendre des comptes à un organe supérieur.

C'est pourquoi la convention institue un organe de surveillance intercantonal constitué de représentantes et de représentants politiques des parties. Les parties sont libres d'y déléguer la personne de leur choix, conformément à la législation applicable dans leur cas.

On s'est abstenu à dessein d'inscrire dans la convention des prescriptions sur l'organisation et la périodicité des comptes rendus car ces aspects sont du ressort des parties et de leurs législations respectives. La première tâche de l'organe de surveillance intercantonal consistera donc à se constituer et à s'organiser lui-même de manière appropriée.

[25] Cf. ch. 3.2.

Article 4

Le comité directeur[26] se constitue lui-même. Il se compose d'un représentant ou d'une représentante de chacune des parties à la convention. Il appartient à ces dernières de choisir la personne appelée à représenter leurs intérêts au sein du comité. Il est judicieux de choisir pour cela quelqu'un possédant de bonnes connaissances de la matière et du paysage policier. Il serait logique que les membres du comité directeur soient choisis au niveau hiérarchique des commandements de police et des cheffes et chefs de police judiciaire ou de division de police judiciaire.

Le comité directeur a différentes tâches, qui ne sont pas énumérées exhaustivement. Il est responsable de la direction et de la mise en œuvre stratégiques de la convention. Cela inclut en particulier le pouvoir fondamental de choisir les banques de données qui seront exploitées dans le cadre de la convention. Le comité directeur reçoit les demandes d'adhésion à la convention et les avis de dénonciation[27] et il règle les différends[28]. Dans des cas particuliers, c'est-à-dire si le différend porte sur un objet dépassant le cadre de l'application et de l'interprétation de la convention, le comité directeur peut instituer un tribunal arbitral indépendant, dont les décisions sont susceptibles de recours auprès du Tribunal fédéral (art. 189, al. 2 Cst.).

La mission centrale du comité directeur est l'élaboration du règlement d'exploitation des différentes banques de données[29]. Dans l'exercice de cette fonction, il veille au respect et à l'application équilibrée des dispositions de la convention[30]. La répartition des coûts d'une banque de données est réglée exclusivement par les participants entre eux. Le comité directeur ne fait que s'assurer qu'elle est conforme aux dispositions de l'article 14.

Article 5

Si les décisions stratégiques appartiennent au comité directeur, la mise en œuvre opérationnelle au niveau des banques de données incombe aux services centraux, en collaboration avec les services extérieurs. Le service central de chaque banque de données a qualité pour représenter les participants à l'égard des tiers et, si nécessaire, conclure des contrats de licence (y compris pour le service et l'assistance). Le service central est chargé en particulier de l'exploitation de la banque de données. Il accomplit cette tâche en respectant les prescriptions de rang supérieur ainsi qu'en appliquant la convention et le règlement d'exploitation.

---

[26] Cf. ch. 3.3.2.
[27] Cf. art. 17.
[28] Cf. art. 20.
[29] Dans la pratique, le comité directeur déléguera l'élaboration détaillée des règlements d'exploitation au service central de la banque de données concernée, sauf si un corps de police présente d'emblée un projet.
[30] Il lui est interdit d'édicter des règles de droit (cf. note de bas de page 13).

Le service central peut recevoir le concours de services extérieurs. L'organisation concrète et la répartition des tâches sont à définir dans le règlement d'exploitation. Le service central comme les services extérieurs doivent respecter les dispositions légales pertinentes en ce qui concerne le traitement des données.

L'alinéa 4 impose aux participants un devoir de notification. En effet, pour atteindre un niveau de contrôle suffisant en ce qui concerne le traitement des données et la traçabilité, il faut savoir quels collaborateurs et collaboratrices sont autorisés à traiter des données au sein du service central et des services extérieurs.

Article 6

Il est normal que les commandantes et commandants de police soient responsables de la protection et de la sûreté des données dans leur service, que ces informations aient été recueillies à l'interne ou fournies par des tiers. Mais ils ne peuvent assumer cette responsabilité que si les fournisseurs de données («services extérieurs») assument cette même responsabilité de leur côté et sont tenus de les aviser lorsque leurs données ne peuvent plus donner lieu à une utilisation licite ou cessent d'être exactes[31].

Article 7

Le règlement d'exploitation est la pièce maîtresse du dispositif au niveau de la banque de données. Une partie à la convention ne devient un participant à une banque de données, avec les droits et les devoirs associés, qu'après en avoir accepté le règlement d'exploitation.

La compétence d'adhérer à une banque de données est régie par le droit du participant. Il lui incombe donc d'obtenir les approbations ou les délégations nécessaires avant d'adhérer.

Les délais d'effacement des données sont régis par les articles 13 et 16 (al. 2, lit. *g*) tandis que les modalités de détail et les procédures d'effacement sont à définir dans le règlement d'exploitation.

Article 8

Alinéa 1: les banques de données contiennent des informations policières au sens fonctionnel. Ce qui est déterminant, c'est que les données soient recueillies aux fins du travail de police et non pas qu'elles soient saisies formellement par un corps de police. La disposition est formulée de façon à pouvoir englober aussi les renseignements émanant des polices communales, par exemple. Il est important également que des organisations qui ne sont pas des polices au sens formel, notamment le Corps des gardes-frontière, puissent adhérer à la convention et alimenter les banques de données. Il est exclu en revanche de recueillir des

[31] Lire aussi le commentaire des art. 10 et 16.

données non policières, par exemple des informations provenant de services de renseignement en Suisse et à l'étranger.

Alinéa 2: les données de base relatives à un incident sont en général établies et validées relativement vite. En revanche, les informations concernant les auteurs et les relations entre les cas sont souvent très fragmentées. L'énumération des données pouvant être traitées permet de collecter les données éparses et, le moment venu, de les assembler pour former un tout cohérent.

Alinéa 2, lettre *b*: les moyens utilisés incluent, dans les cas relevant de la cybercriminalité, le matériel informatique, les logiciels et les programmes malveillants.

Alinéa 2, lettre *c*: les auteurs sont au centre de l'intérêt. Il faut pouvoir réunir des informations fragmentaires. Outre les données personnelles courantes, il est possible d'enregistrer des numéros d'identification tels que les numéros de passeport et les numéros personnels. En effet, ces identifiants sont des constantes alors que les noms peuvent être changés tout à fait légalement dans un grand nombre de pays. En plus des adresses de domicile classiques, les adresses électroniques comme les adresses IP, les URI[32], les adresses électroniques, les noms utilisés sur les réseaux sociaux et les données d'accès aux comptes (y compris biométriques) revêtent une importance croissante pour identifier des personnes. Par données d'accès biométriques, on entend les yeux, les oreilles, les empreintes digitales, les données de reconnaissance faciale et les évolutions de ces technologies.

Alinéa 2, lettre *d*: les informations concernant les personnes lésées énumérées dans cette disposition sont limitées. La présente convention n'autorise pas à établir des interconnexions avec des données plus complètes des cantons ou de la Confédération.

Alinéa 2, lettre *h*: les images en lien avec l'incident incluent les clichés pris par des radars, les images représentant des outils particuliers utilisés pour commettre le délit, des symboles ou les objets dérobés ainsi que les portraits-robots.

Alinéa 2, lettre *j*: le profil d'ADN n'est pas important en soi pour établir un lien avec un incident. Mais il faut avoir la possibilité d'établir un lien entre différents incidents au moyen des numéros de contrôle de processus faisant référence à des profils d'ADN enregistrés sous une forme anonymisée dans les systèmes.

[32] Un *Uniform Resource Identifier* (URI) est une chaîne de caractères servant à identifier une ressource physique ou abstraite. Les URI sont utilisées pour désigner des ressources sur Internet (comme des pages Internet, d'autres types de fichiers, des services Web mais aussi les destinataires de courriels p. ex.). Il existe deux types d'URI: les URL (*Uniform Resource Locator*) et les URN (*Uniform Resource Name*). Schématiquement, une URL indique où se trouve quelque chose (et comment on y arrive) tandis qu'une URN décrit ce qu'est l'objet. À l'origine, les URL étaient le seul type d'URI, raison pour laquelle l'abréviation URL est souvent employée pour URI.

Alinéa 2, lettre *k*: cette disposition fait actuellement référence aux numéros IBAN, aux adresses Bitcoin, aux comptes en monnaie virtuelle Seeds, aux portefeuilles pour cryptomonnaies, etc. La convention préfère une formulation générale à des désignations explicites car ces dernières évoluent extraordinairement vite.

Article 9

Par rapport aux évaluations réalisées de manière traditionnelle par des analystes, l'évaluation automatique des données par voie électronique constitue une atteinte beaucoup plus importante à la maîtrise des données, raison pour laquelle elle doit reposer sur une habilitation expresse dans la présente convention, conformément aux principes de la protection des données.

Cette disposition concrétise l'article 8, alinéa 1: elle précise que la notion de traitement des données comprend en particulier l'échange, l'enregistrement, la mise en relation et l'analyse de données.

Chacune des parties à la convention est tenue d'appliquer individuellement à ses données les règles figurant dans la directive de l'Union européenne 2016/680. Il est donc inutile de prévoir une réglementation spécifique dans la présente convention.

L'alinéa 2 a été formulé de manière à permettre l'externalisation de la sauvegarde physique des données, comme cela se pratique à l'heure actuelle avec un certain nombre d'applications de police. La législation du canton où la banque de données a son siège ou, si le service central de la banque de données est un service fédéral, la législation fédérale détermine les conditions dans lesquelles il est possible de recourir à cette possibilité[33] ou si cela requiert une adaptation de la convention. À noter que l'option d'une externalisation n'est pas envisagée dans les travaux de projet en cours sur PICAR[34].

Article 10

Cette disposition prévoit que l'accès total aux banques de données n'est accordé qu'à un petit cercle d'utilisatrices et d'utilisateurs pour chaque banque de données.

Seuls les produits issus des banques de données (analyses, rapports) sont accessibles à un cercle de personnes plus large, qui est toutefois limité au personnel des corps de police participants et du CGFR ou d'autres services appropriés de la Confédération (lire le commentaire de l'art. 17, al. 1).

Les données validées fournies à une banque de données continuent bien sûr de figurer dans la banque de données du service ou de l'autorité qui les a communiquées. Elles ne peuvent

[33] P. ex. que le serveur soit implanté en Suisse.
[34] Cf. ch. 3.2.2.

être modifiées[35] que par leur fournisseur, qui a la responsabilité de leur licéité et de leur exactitude (art. 6, al. 2). *A contrario*, les autres services et autorités ne sont pas habilités à les modifier. Le fournisseur doit donc apparaître clairement en tout temps dans les caractéristiques des données.

Le service central et les services extérieurs peuvent compléter et mettre en relation les données contenues dans leur banque, toujours en indiquant quel service a effectué le traitement.

Les procédures de modification et la journalisation des modifications sont des aspects techniques. Elles doivent donc être régies dans le règlement d'exploitation et le concept SIPD.

Article 11

Alinéa 1: pour ne laisser planer aucune incertitude sur le droit applicable et simplifier les processus, les nouvelles banques de données seront régies par une seule législation, celle du canton où est sis le service central de la banque de données. Cela concerne à la fois le droit de la protection des données et le droit procédural ou le droit de la responsabilité qui y sont associés. Le droit applicable détermine en outre la compétence de l'organe de surveillance de la protection des données. Les informations demeurant dans les systèmes de police des cantons ou de la Confédération restent bien entendu soumises à la législation du lieu.

Alinéa 2: la licéité de la saisie de données est régie par le droit applicable au participant qui fournit les données. Les lois sur la police ne sont pas identiques d'un canton à l'autre. Par conséquent, la licéité d'une saisie de données est examinée selon le droit applicable à cette saisie, et non pas selon le droit du service central.

Article 12

Alinéa 1: la procédure applicable aux demandes d'information, de consultation ou de rectification est régie par le CPP ou par la législation sur la protection des données, selon le moment où la demande est présentée. Si la procédure est régie par la législation sur la protection des données, c'est celle du siège du service central qui s'applique.

Alinéa 2: le traitement des demandes incombe au service central. Celui-ci accomplit ce travail en concertation avec les participants qui ont fourni les données car il est possible qu'il n'ait pas connaissance de tous les motifs justifiant que la communication ou la rectification de données soit limitée, différée ou refusée (p. ex. tactique d'investigation).

Dans quelle mesure le service central peut-il procéder lui-même ou doit-il faire procéder par le fournisseur des données à une suppression ou à une rectification? La réponse à cette

[35] Une suppression constitue une modification.

question varie selon la banque de données et elle est fixée dans le règlement d'exploitation. L'exécution de la suppression ou de la rectification incombe toutefois au service central.

Alinéa 3: les motifs limitant une consultation découlent de la législation sur la protection des données du canton ou de la Confédération. Là encore, c'est le droit du siège du service central qui s'applique. Bien que les lois sur la protection des données aient des formulations très analogues, il est possible en théorie que les règles régissant le droit de consultation ne soient pas identiques dans tous les cantons ni au niveau fédéral. De telles divergences devraient toutefois rester rares et peu substantielles dans la pratique.

La législation fédérale peut en outre fournir des motifs de limitation supplémentaires.

Article 13

La réglementation des délais d'effacement est nécessaire pour des raisons de protection des données. Mais elle est utile également pour gérer les données et optimiser l'exploitation des systèmes de suivi et d'analyse de la situation.

Alinéa 1, lettre *a*: les données doivent être effacées dès qu'elles deviennent inutiles pour le traitement. La disposition fixe en outre un délai maximal absolu de dix ans après lequel les données doivent être effacées dans tous les cas.

Alinéa 1, lettre *b*: si les données concernent des incidents clairement liés, c'est le dernier ajout au tableau d'ensemble qui détermine le début du délai. Cette disposition évite que certains incidents soient supprimés prématurément de la banque de données alors qu'ils auraient été utiles pour évaluer la situation ou élucider un cas par la suite. Il est en outre possible de saisir à nouveau des incidents particulièrement pertinents s'ils sont encore en cours de traitement chez un participant car la présente disposition est sans effet sur les délais d'effacement dans les systèmes de police des cantons ou dans les systèmes de la Confédération.

Alinéa 1, lettre *c*: s'il est possible de lever les soupçons qui pèsent sur une personne, il n'y a pas de raison de conserver ses données plus longtemps. Cela contreviendrait au principe de la proportionnalité.

Alinéa 2: pour protéger les victimes, les données relatives aux personnes lésées doivent être supprimées des banques de données dès que le but du traitement le permet. Cela signifie d'une part que le lien entre les données et les personnes est supprimé d'office dès qu'il est possible de travailler avec des données anonymisées et, d'autre part, que toutes les données concernant les personnes lésées sont effacées dès que le but du traitement le permet.

Article 14

La convention fixe les principes de financement qui s'appliqueront à tous les systèmes de suivi et d'analyse de la situation exploités en commun[36].

L'exploitation de ces systèmes entraîne des coûts d'infrastructure, d'exploitation et de licence, qui doivent être supportés par les participants utilisant les systèmes (al. 1)[37]. L'alinéa 2 régit la répartition des coûts d'exploitation du service central et du service de surveillance de la protection des données de chaque banque de données[38]. Chaque participant à une banque de données doit prendre à sa charge une partie de ces coûts. Les modalités concrètes de la répartition doivent être adaptées à chaque système. La convention propose quatre clés de répartition possibles, les deux dernières pouvant être complétées par une contribution de base répartie à parts égales entre les participants afin d'éviter qu'un gros participant ne supporte une partie disproportionnée des charges (al. 3). La liste des clés de répartition est exhaustive. L'application d'autres modalités requiert donc une modification de la convention.

Les coûts peuvent être répartis entre les participants cantonaux, d'une part, et les participants de la Confédération (et de l'étranger le cas échéant), d'autre part, selon un ratio 70/30, comme prévu aux articles 11 et 12 de la Convention du 10 novembre 2011 entre la Confédération et les cantons visant à harmoniser l'informatique policière en Suisse (lit. *a*). Dans ce cas, les cantons se partagent leur contribution au pro rata de leur population résidante permanente connue au moment de la facturation.

Il peut être adéquat de répartir les contributions au pro rata du nombre de participants (lit. *b*) ou d'appliquer la clé de répartition éprouvée de la Conférence des directrices et directeurs des départements cantonaux de justice et police (CCDJP), qui reposerait alors sur la population résidante permanente des participants connue à la date d'entrée en vigueur de la convention (lit. *c*). La quatrième et dernière possibilité consiste à calculer la contribution en se basant sur le volume des données traitées par les participants (lit. *d*).

Il appartient aux participants à chaque banque de données de fixer la clé de répartition applicable et de lui conférer un caractère obligatoire en l'inscrivant dans le règlement d'exploitation de la banque de données. Les participants choisissent la clé de répartition la mieux adaptée aux spécificités concrètes du système de suivi et d'analyse concerné.

---

[36] Cf. chap. 3.

[37] Il n'y a pas de coûts de licence pour PICAR, qui est mis à disposition gratuitement par ses développeurs, l'Université de Lausanne et la Police cantonale vaudoise.

[38] Les coûts du service de surveillance de la protection des données ne peuvent être répercutés sur les participants que si une base légale le prévoit expressément dans la législation du canton où est sis ce service. À notre connaissance, ce n'est actuellement le cas dans aucun canton.

La compétence des participants pour approuver la clé de répartition choisie et régler les contributions dues est naturellement régie par la législation applicable dans chaque cas[39].

Article 15

L'alinéa 1 prévoit la possibilité de sortir d'une banque de données. La sortie doit avoir lieu de manière ordonnée. Il faut ménager un délai suffisant pour mener à bien cette procédure; six mois sont considérés comme suffisants.

Les alinéas 2 et 3 disposent que les droits (p. ex. utilisation de la banque de données) et les devoirs (p. ex. obligation de participer aux coûts) attachés à la qualité de participant à une banque de données prennent fin au moment où la dénonciation prend effet. Le départ d'un participant peut avoir des conséquences financières, mais la convention précise que les dépenses de biens et services et de personnel ne donnent en principe pas lieu à remboursement.

Les divergences qui pourraient surgir en relation avec un départ rentrent dans le champ des dispositions relatives au règlement des différends (art. 20 en rel. avec art. 4, al. 1).

Article 16

Alinéa 1: lorsqu'un participant quitte une banque de données, les données qu'il a fournies sont effacées. Les participants sont responsables de la licéité et de l'exactitude des données qu'ils enregistrent[40]. Le participant qui quitte une banque de données perd l'accès à ses données et donc la possibilité de les corriger s'il apparaît qu'elles ne sont plus exactes. Il devient ainsi impossible de garantir que les informations en question sont licites et exactes. Il est donc logique que les données apportées par un participant soient effacées lorsque ce participant quitte la banque de données, dans la mesure où elles ne sont pas en lien avec un incident saisi par un autre participant.

Il découle de cette disposition que les banques de données doivent être configurées de manière à permettre l'effacement des données d'un participant. Le système PICAR remplit cette exigence.

Alinéa 2: lorsqu'une banque de données est dissoute dans son entièreté, tous les jeux de données qu'elle contient sont effacés. La procédure technique d'effacement doit être conçue de façon à ce que les informations soient définitivement effacées, sans pouvoir être restaurées. Cela est indispensable pour protéger les données personnelles contre un traitement illicite. Le coût éventuel de l'effacement est pris en charge selon la clé de répartition de la banque de données. Les règles détaillées à appliquer figurent dans le règlement d'exploitation (cf. art. 7, al. 2, lit. *e*).

[39] Lire le commentaire de l'art. 7.
[40] Lire le commentaire de l'art. 6.

Article 17

L'alinéa 1 précise qui peut adhérer à la convention. Il s'agit de tous les cantons et des services appropriés de la Confédération. Comme la présente convention a pour but premier de faciliter la coopération entre les cantons dans le domaine de la police aux fins indiquées (art. 1), il est logique que l'ensemble des cantons puissent y adhérer.

Mais il existe aussi des organisations non cantonales qui s'efforcent de lutter efficacement contre la délinquance sérielle. Ces organisations doivent elles aussi pouvoir adhérer à la convention. L'article 17, alinéa 1 limite cette possibilité aux services appropriés de la Confédération. Ainsi, seuls des services fédéraux peuvent devenir parties à la convention[41], mais encore faut-il qu'ils soient appropriés, c'est-à-dire qu'ils puissent contribuer à améliorer la lutte contre la délinquance sérielle. On pense par exemple au Corps des gardes-frontière ou à la Police judiciaire fédérale.

La disposition précise que l'adhésion à la convention est valable avec effet immédiat. Cela signifie que les futures parties ont accompli, avant d'adhérer, toutes les formalités nécessaires au niveau cantonal ou fédéral (p. ex. décision du législatif, publication officielle).

Les parties à la convention peuvent non seulement sortir d'une banque de données (art. 15), mais aussi dénoncer la convention. Dans ce cas également, la convention prévoit un préavis de six mois pour la fin d'une année civile.

Article 18

La présente convention entre en vigueur dès que l'adhésion de deux parties au moins a été validée dans les formes prévues par la législation applicable. Les conditions à remplir sont déterminées par le droit du canton ou le droit fédéral.

Les adaptations matérielles et les modifications de la convention requièrent l'approbation de toutes les parties (al. 2). Le droit applicable pour chaque partie détermine les modalités à respecter pour obtenir ce consentement.

Article 19

Aux termes de l'article 48, alinéa 1 Cst., les cantons peuvent conclure des conventions entre eux et créer des organisations et des institutions communes. Ils peuvent notamment réaliser ensemble des tâches d'intérêt régional. La Confédération peut y participer dans les limites de ses compétences (art. 48, al. 2 Cst.). Les conventions intercantonales ne doivent être contraires ni au droit et aux intérêts de la Confédération, ni au droit des autres cantons. Elles doivent être portées à la connaissance de la Confédération (art. 48, al. 3 Cst.).

[41] La possibilité pour la Confédération de participer à un concordat est prévue à l'art. 48, al. 2 Cst.

[Traduction]

Selon l'article 56, alinéa 2 Cst., les traités conclus par les cantons avec l'étranger ne doivent être contraires ni au droit et aux intérêts de la Confédération, ni au droit d'autres cantons. Avant de conclure un traité, les cantons doivent en informer la Confédération. Aux termes de l'article 56, alinéa 3 Cst., les cantons peuvent traiter directement avec les autorités étrangères de rang inférieur; dans les autres cas, les relations des cantons avec l'étranger ont lieu par l'intermédiaire de la Confédération. Selon l'article 172, alinéa 3 Cst., l'Assemblée fédérale approuve les conventions que les cantons entendent conclure entre eux et avec l'étranger, mais seulement lorsque le Conseil fédéral ou un canton élève une réclamation.

L'article 19 de la présente convention, qui a une valeur déclaratoire, rappelle explicitement ces obligations constitutionnelles, qui concernent à la fois l'entrée en vigueur de la convention et toutes les modifications qui pourraient lui être apportées par la suite.

Article 20

La présente convention ne devrait pas donner lieu à des litiges et, si litiges il devait y avoir, ils pourront très certainement être réglés à l'amiable. Elle confère néanmoins au comité directeur la compétence de régler les différends entre les parties (en prévoyant une possibilité de recours devant le Tribunal fédéral; lire le commentaire de l'art. 4).

Article 21

Comme les règles régissant la responsabilité ont un caractère législatif, elles sont définies dans la convention. Elles sont inspirées des dispositions en la matière prévues dans le concordat policier de la Suisse du Nord-Ouest. Du fait de leur mention expresse dans la convention, elles s'imposent à toutes les parties.

L'alinéa 2 garantit que les citoyennes et les citoyens concernés ne subissent pas d'inconvénients découlant de l'institution par la convention d'une organisation particulière chargée de traiter des données.

Bâle, le 14 juin 2019
Concordat policier de la Suisse du Nord-Ouest