KKPKS CCPCS
Konferenz der kantonalen Polizeikommandantinnen und -kommandanten
Conférence des commandantes et des commandants des polices cantonales
Conferenza delle e dei comandanti delle polizie cantonali

Generalsekretariat

Convention intercantonale sur l'échange de données à des fins d'exploitation de plates-formes de recherche et de systèmes de bases de données communs

Rapport d'évaluation relatif à la consultation « POLAP »

Secrétariat général CCPCS, Maison des cantons, Speichergasse 6, 3011 Berne
Tél. +41 (0)31 512 87 20, info@kkpks.ch

Berne, le 23 mars 2024

Convention intercantonale sur l'échange de données à des fins d'exploitation de plates-formes de recherche et de systèmes de bases de données communs

Rapport d'évaluation relatif à la consultation « POLAP »

Table des matières

Glossaire

Acronyme / abréviation	**Définition**
Art.	Article
LSIP	Loi fédérale sur les systèmes d'information de police de la Confédération du 13 juin 2008, RS 361
Cst.	Constitution fédérale de la Confédération suisse du 18 avril 1999, RS 101
LTF	Loi sur le Tribunal fédéral du 17 juin 2005 RS 173.110
PFPDT	Préposé fédéral à la protection des données et à la transparence
LA	Loi d'application
DFJP	Département fédéral de justice et police
fedpol	Office fédéral de la police fedpol
GUI	Interface graphique utilisateur (angl. *Graphical User Interface*)
CSI	Centre de services informatiques
POCA	Police cantonale
OAB	Escroquerie au placement en ligne
PICSEL	PICSEL est une base de données spécifiquement destinée à l'analyse des renseignements sur la cybercriminalité (système de collecte d'informations supracantonal visant notamment à dégager des liens entre les cas et à identifier des séries parmi un nombre sans cesse croissant de cyberdélits).
SPC	Statistique policière de la criminalité
POLAP	Plate-forme de recherche policière
LPol	Loi cantonale sur la police
TIP	Technique et informatique policères Suisse
Convention TIP	Convention entre la Confédération et les cantons sur l'harmonisation et la mise à disposition commune de la technique et de l'informatique policières en Suisse (convention TIP)
RIPOL	Système de recherches informatisées de police
RS	Recueil systématique du droit fédéral
VOSTRA	Casier judiciaire informatisé
SYMIC	Système d'information central sur la migration

Consultation « POLAP »

1. Résumé

La procédure de consultation « POLAP » de la CCDJP relative à la « convention intercantonale sur l'échange de données à des fins d'exploitation de plates-formes de recherche et de systèmes de bases de données communs » s'est déroulée du 23 novembre 2023 au 23 février 2024.

Des prises de position ont été reçues de la part du PFPDT, de fedpol, de l'Office fédéral de la douane et de la sécurité des frontières, de privatim, de l'association Société numérique, de la Conférence des directrices et directeurs de la sécurité des villes suisses et du Parti socialiste suisse ainsi que des cantons de Lucerne, Zurich, Valais, Uri, Bâle-Campagne, Fribourg, Vaud, Genève, Berne, Thurgovie, Schwyz, Neuchâtel, Soleure, Obwald, Glaris, Nidwald, Argovie, Jura, Appenzell Rhodes-Intérieures, Tessin, Schaffhouse, Appenzell Rhodes-Extérieures et Bâle-Ville.

La création d'une convention intercantonale continue de bénéficier d'un large soutien. Seul un canton estime que la mise en œuvre d'une convention intercantonale n'est pas viable, et seul un autre canton a indiqué que, en raison de l'absence de certaines dispositions, il ne saurait approuver un tel projet de concordat.

Le souhait d'une réglementation au niveau national a été exprimé à plusieurs reprises. En effet, la motion 23.4311 visant à créer une base constitutionnelle pour une réglementation fédérale de l'échange de données de police au niveau national, déposée par la Commission de la politique de sécurité du Conseil national, a été explicitement saluée. Le PFPDT est lui aussi d'avis que le but de la convention ne saurait être atteint de manière légale et crédible que par l'introduction d'une nouvelle disposition dans la Constitution fédérale. Une modification constitutionnelle serait soumise au référendum et à une votation populaire fédérale, ce qui donnerait une légitimité démocratique plus large à l'échange de données policières tel qu'il est envisagé.

Sur le fond, de nombreuses prises de position ont fait état de préoccupations concernant la protection des données et les droits fondamentaux. La question de savoir si le projet de loi respecte le principe de précision de la base légale et le principe de proportionnalité, tels qu'ils sont inscrits dans la Constitution, a été soulevée. De même, des voix se sont élevées pour souligner que l'échange automatisé de données par procédure d'appel, de même que tout système de base de données commun entre les cantons ou entre ceux-ci et la Confédération seraient contraires à la répartition, telle que définie par l'État, des compétences en matière de police.

Plusieurs remarques ont également été émises concernant les lois cantonales sur la police récemment révisées ou en cours de révision et qui, déjà, prévoient une base légale pour l'échange de données avec d'autres cantons.

Des remarques et des questions ont été formulées concernant le droit applicable et la responsabilité en matière de protection des données dans le cadre des systèmes d'information à mettre en place en vertu du présent concordat. La révision du texte du concordat et du rapport explicatif doit permettre de clarifier ces questions.

2. Analyse des résultats de la consultation « POLAP »

But

En ce qui concerne notamment l'objet et le but (art. 1) ainsi que le champ d'application (art. 3), la CCPCS constate que les formulations, larges et ouvertes, englobent presque tous les domaines d'activité de la police et que, par conséquent, la convention n'est pas conforme aux principes de légalité, de précision de la base légale et de proportionnalité. Il est donc douteux que le projet, dans sa forme actuelle, puisse soutenir une procédure de contrôle des normes. Une autre question a été posée : existe-t-il, sur tout le champ du concordat, un intérêt public prépondérant qui justifierait les atteintes aux droits fondamentaux qui résultent de l'échange de données (art. 36, al. 2, Cst.) ?

Pour respecter le principe de précision de la base légale et limiter le but de la convention, la CCPCS étudie actuellement l'option consistant à lier la condition d'une requête sur POLAP à la gravité de l'infraction. Concrètement, plusieurs catalogues d'infractions offrant un rapport équilibré entre le besoin de consultation et l'atteinte aux droits fondamentaux sont à l'étude. Si cette solution était adoptée, il s'ensuivrait qu'une autorité de police ne pourrait consulter des données via POLAP que dans certains cas d'infractions. Le catalogue des infractions déterminerait le droit d'accès aux données selon le critère de la gravité. Le droit d'une autorité requérante de traiter ultérieurement les informations obtenues via POLAP dépend de la base légale en vigueur dans le canton dont elle relève.

Du point de vue des droits fondamentaux, l'introduction d'une liste d'infractions n'autorisant la consultation que pour certaines infractions, éventuellement les plus graves, signifierait que les conditions d'une atteinte aux droits fondamentaux deviendraient ainsi plus strictes. Une telle solution est également envisagée par la CCPCS pour les systèmes de base de données communs.

Partage constitutionnel des compétences

Se fondant sur certaines prises de position, la CCPCS a conclu qu'en raison de son large champ d'application, le concordat ne respectait pas le partage des compétences prévu par la Constitution, qui attribue les compétences policières en premier lieu aux cantons (art. 3 et 57 Cst.). La répartition des tâches entre la Confédération et les cantons, telle que définie par la Constitution, en matière de prévention des infractions, de lutte contre celles-ci et d'enquête, serait ainsi brouillée.

La CCPCS est d'avis qu'en vertu de la souveraineté cantonale en matière policière (art. 3 Cst.), les cantons ont la compétence de légiférer dans ce domaine. Ils sont souverains dans

l'accomplissement de leurs tâches dans ce domaine, en respectant les limites du cadre légal. La Confédération ne dispose que des compétences qui lui sont conférées par la Constitution.

La Confédération et les cantons ont en commun le devoir d'assurer la sécurité du pays (art. 2, al. 1 Cst.) et de s'entraider dans l'accomplissement de leurs tâches (art. 44 Cst.). La CCPCS en conclut qu'il est tout à fait conforme à la Constitution de mettre en place et d'exploiter des plate-formes de recherche gérées par la Confédération aux fins d'échange de données entre les systèmes sources cantonaux ainsi que des systèmes de base de données communs. D'une part, la Confédération soutient de cette manière les cantons dans l'accomplissement de leurs tâches de police. D'autre part, en vertu de leur souveraineté policière, les cantons peuvent aussi faire appel à la Confédération au titre de l'exécution de leurs tâches de police et mettre en place des systèmes de base de données communs moyennant la création des bases juridiques correspondantes. En d'autres termes, le fait que les cantons puissent collaborer avec la Confédération lorsqu'ils le jugent opportun pour l'accomplissement de leurs tâches découle de leur souveraineté policière. Le fait que la Confédération et les cantons prennent part, dans leurs cadres respectifs, à des plate-formes de recherche et à des systèmes de bases de données communs ne signifie pas pour autant qu'il y ait une contradiction avec le partage constitutionnel des compétences. C'est à partir des bases juridiques respectives que l'on peut déterminer si la Confédération ou les cantons sont autorisés à stocker et à consulter des données policières sur des plate-formes de recherche ou des bases de données communes.

La CCPCS conclut que, compte tenu de ce qui précède, l'utilisation de l'expression « espace national de données de police suisse » est trompeuse et doit être proscrite dans le futur texte du concordat. Cette expression a été reprise dans le projet à partir de la motion Eichenberger du 9 décembre 2019 dans le but de faire apparaître le lien entre celle-ci et le concordat. Il ne s'agit en aucun cas de créer un espace national unique de données policières censé permettre à toutes les autorités de police d'accéder en bloc et à tout moment à l'ensemble des données policières existantes. L'objectif du concordat est de créer les bases juridiques permettant aux autorités de police, en cas de besoin avéré et dans le respect des principes de l'État de droit, de mettre en place et d'exploiter des plate-formes de recherche et des systèmes de base de données communs afin d'accomplir leurs tâches de police de manière plus efficace et plus économe en ressources, notamment par l'exploitation ciblée de technologies modernes.

<u>Besoin en matière de plates-formes de recherche policière et de systèmes de base de données communs</u>

La CCPCS souligne que la question d'un échange intercantonal de données n'est pas nouvelle, celle-ci étant discutée dans les cantons depuis longtemps déjà. Plusieurs travaux, par ailleurs, ont déjà porté sur cette question. Le 2 avril 2009 déjà, l'Accord intercantonal de la coopération assistée par ordinateur des cantons lors de l'élucidation des délits de violence (Concordat ViCLAS) était signé. L'extension du concordat intercantonal instituant des mesures contre la violence lors de manifestations sportives est entrée en vigueur en février 2012. Conformément à l'art. 24a de la loi fédérale instituant des mesures visant au maintien

de la sûreté intérieure (RS 120), fedpol gère un système d'information central dans lequel sont consignées les mesures prises dans le cadre du concordat.
Du fait de la structure fédéraliste de la Suisse, les systèmes intercantonaux ou nationaux constituent toutefois l'exception. Actuellement, outre les systèmes nationaux (RIPOL, SYMIC, index national de police, VOSTRA etc.), chaque corps de police dispose, en particulier, d'un système propre de traitement des affaires qui couvre l'ensemble des opérations policières.

Ce n'est que dans des cas isolés qu'une autorité de police est habilitée à consulter les bases de données policières d'autres collectivités publiques (par ex. dans le domaine des enquêtes de police judiciaire selon l'art. 10, al. 4 LSIP). La consultation des données doit en principe se faire de manière sérielle et sur demande individuelle auprès de chaque autorité concernée. Toutefois, vu les formes d'infraction actuelles, la CCPCS estime qu'un échange automatisé de données s'avère nécessaire pour assurer l'efficacité de la lutte contre la criminalité, de sa prévention et des enquêtes, comme en témoignent les exemples ci-après.

Opérations de police visant une personne donnée : La police cantonale bernoise est régulièrement confrontée à des personnes qui mettent en danger l'intégrité psychique, physique ou sexuelle de tiers. Cette menace peut être dirigée contre des personnes de l'environnement privé, professionnel ou scolaire, mais aussi contre des membres des autorités, de services administratifs, d'institutions ou d'entreprises. De telles personnes apparaissent souvent dans plus d'un canton (du fait d'un lieu de travail ou de contacts situés dans d'autres cantons que celui de résidence). Dans les situations de danger imminent, notamment, il est crucial de pouvoir prendre connaissance sans délai de toutes les opérations de police concernant la personne en question afin de pouvoir procéder à une évaluation pertinente de la situation. C'est la seule façon d'assurer que les mesures nécessaires sont prises à temps.
« Personne menaçante » : Dans le canton de Berne, une personne a gravement menacé une présidente de tribunal, ce qui a fait craindre une escalade imminente de la violence. La personne menaçante réside en dehors du canton tandis que son lieu de travail se trouve dans un troisième canton. Dans chacun des cantons concernés, la personne s'est fait connaître par des menaces graves et des comportements parfois violents. Dans un premier temps, tous les cantons ont pris, indépendamment les uns des autres, des mesures de limitation des risques. Ce n'est que dans le cadre d'un examen plus approfondi que les liens sont apparus et que les mesures ont pu être coordonnées. La prise en compte rapide de tous les incidents connus est essentielle, en particulier dans de telles situations d'urgence, et peut contribuer à prévenir rapidement les actes de violence. Les possibilités actuelles d'échange de données, face à de telles situations de menace imminente, ne permettent pas d'obtenir ce type d'informations à temps, car le traitement par la police judiciaire n'intervient qu'ultérieurement et les requêtes ne sont traitées qu'avec retard.

Données d'enquête : Face à la réalité complexe de la criminalité, il n'est plus possible de mener des enquêtes dans les limites des structures cantonales. Les groupes criminels agissent à l'échelle intercantonale et souvent internationale. Ce constat est particulièrement évident dans les domaines du cyberespace, de la traite d'êtres humains, du terrorisme et des

infractions contre le patrimoine commises en bande, où les groupes d'auteurs agissent typiquement dans le cadre d'un réseau. Dans de tels cas, l'échange de données d'enquête est essentiel. Les services d'enquête ne peuvent identifier des séries et des corrélations pertinentes que si les données qui les composent sont disponibles.

Homicide : dans un « cold case » extra-cantonal (meurtre d'une prostituée), plusieurs cantons ont été chargés d'établir un profil d'ADN par dépistage de masse. La police cantonale bernoise est compétente en ce qui concerne deux personnes. L'une d'elles est connue de leurs services pour des faits de pornographie violente (fantasmes d'homicide). Vu les circonstances, cette personne aurait été du plus grand intérêt pour le canton concerné par l'affaire. Ce lien n'a toutefois été identifié que lorsque la police cantonale bernoise a procédé à un contrôle de la personne dans le cadre d'un prélèvement de frottis de la muqueuse jugale. Si la police compétente a découvert le nom de la personne concernée, c'est uniquement sur la base de communications de la population après un reportage dans l'émission « *Aktenzeichen XY Ungelöst* ».
Lorsque l'on veut établir des liens dans de tels cas – ou en relation avec d'autres types d'infractions – on est obligé (en l'état actuel des choses) de soumettre une demande aux corps de police de Suisse (diffusion nationale). Malheureusement, il n'est pas rare que les retours d'information soient incomplets ou même que l'on oublie de les donner. Le fait que l'autorité répondante ne connaisse pas l'affaire et ne sache donc pas quelles informations sont pertinentes pour l'enquête joue certainement un rôle à cet égard.

Cybercriminalité : À la différence des infractions commises dans l'espace matériel, les infractions relevant de la cybercriminalité ont un impact élevé à l'échelle mondiale. Autrement dit, une attaque affecte généralement un nombre incalculable de personnes dans le monde entier, ou du moins dans une région donnée. Il en résulte des indicateurs numériques (par exemple des adresses IP, des noms de domaine, des transactions cryptographiques, des signatures de logiciels malveillants, des liens d'hameçonnage, etc.) qui, lorsqu'ils sont placés dans un contexte global, forment, en quelque sorte, une empreinte qui permet d'identifier l'auteur de l'infraction. L'échange automatisé de tels indicateurs pourrait permettre d'éviter des enquêtes parallèles. À l'heure actuelle, les cas ne peuvent être traités qu'individuellement, ce qui entraîne un énorme surcroît de travail.
Suite à une dénonciation pénale pour escroquerie au placement en ligne, l'identifiant numérique (adresse IP) de l'infrastructure utilisée par les auteurs de l'infraction (accès à distance, envoi de courriers électroniques et plate-forme commerciale exploitée par les auteurs) a permis de reconnaître et de saisir le serveur et d'identifier les auteurs de l'infraction. Dans un autre cas d'escroquerie au placement en ligne, seule la technologie du site et le certificat des plates-formes de négoce exploitées par les auteurs ont pu être identifiés. L'échange automatisé de ce type de données permettrait à l'avenir d'identifier plus tôt les liens entre les deux affaires et d'obtenir ainsi des informations précieuses permettant d'identifier les auteurs et, le cas échéant, de prévenir d'autres cas.

Cybercriminalité : Pour dresser un tableau de la situation au niveau national, il est indispensable de disposer d'une base de données nationale. En l'absence de système de base de

données commun, une autorité de police ne peut pas en savoir plus que ce qui se produit dans son propre canton.
Une telle base de données est également nécessaire pour pouvoir déterminer de manière fiable si l'auteur d'une infraction fait également l'objet d'enquêtes dans d'autres cantons. À l'origine d'une procédure dans le domaine de la cybercriminalité, il y a presque toujours un groupe d'auteurs inconnu, et aucun extrait du casier judiciaire ne permet de savoir si d'autres procédures sont en cours ou closes dans d'autres cantons ou au niveau de la Confédération. Cela entraîne des doublons (p. ex. administration des preuves reproduite à l'identique par différents cantons, doublement des charges de personnel etc.), rendant difficile et longue la clarification de la question de la compétence. Un bon exemple à cet égard est celui d'un groupe de rançongiciels qui attaque et extorque de l'argent à un grand nombre d'entreprises en Suisse.
Là encore, il n'est guère possible de comparer les caractéristiques de référencement (p. ex. adresses cryptographiques, IP ou électroniques des auteurs, numéros de téléphone etc.) au niveau national et de rattacher (indépendamment du phénomène) des cas individuels à une série d'infractions commises par le même auteur. Étant donné que les cas individuels n'offrent généralement guère de pistes d'investigation, cette situation a pour conséquence qu'ils sont suspendus ou classés (ou rapportés aux archives). En revanche, si les cas pouvaient être identifiés comme faisant partie d'une série d'infractions en raison de la concordance des caractéristiques de référence et si les procédures correspondantes étaient unifiées, les chances d'aboutir à des pistes d'enquête prometteuses et, par conséquent, d'identifier les auteurs et de les traduire en justice, s'en trouveraient considérablement accrues.

Infractions économiques : La base de données dite « OAB » a pour dénomination « PICSEL » et est gérée par les polices cantonales d'Argovie et de Genève. Depuis environ deux ans, les caractéristiques de référencement de l'ensemble des rapports OAB en Suisse y sont recensées. Les données sont analysées en continu et discutées régulièrement dans le cadre des séances OAB du point de contact unique (PCU), qui réunissent des représentants de tous les cantons et sont organisées par le réseau national de soutien aux enquêtes dans la lutte contre la criminalité informatique (NEDIK).
PICSEL est, proprement dit, un prototype. Grâce à cette base de données, on a pu constater que dans le domaine de la « cybercriminalité économique » en série, des économies de ressources considérables peuvent être réalisées dans une première phase si l'on se limite à la collecte de données. PICSEL permet ensuite de rassembler « d'un simple clic » toutes les informations relatives aux procédures correspondant à certaines caractéristiques de référencement à l'échelle nationale (adresses IP, numéros de téléphone, alias de démarcheurs téléphoniques, numéros de compte, adresses cryptographiques etc.). Actuellement, des procédures collectives de ce type sont en cours dans plusieurs cantons. En termes de coordination et de coopération internationales, les autorités de police sont également en bonne position.

PICSEL est cependant trop limitée sur certains points. La conception devrait être largement développée, notamment en ce qui concerne l'étendue des infractions à intégrer (actuellement limitée aux OAB), l'analyse des données (très « bricolée »), l'échange de données au

niveau intercantonal et international (aucune compétence n'y étant définie) et l'efficacité (pas d'utilisation dans le cadre de mesures de prévention et en matière de démantèlement de réseaux criminels). Les données relatives à toutes les infractions économiques relevant de la cybercriminalité (selon la terminologie de la statistique policière de la criminalité) ainsi qu'aux procédures relatives au blanchiment d'argent (notamment en ce qui concerne les passeurs d'argent) doivent être réunies dans une base de données moderne et rendues accessibles dans le contexte d'une analyse professionnelle. Il convient également de mettre en place un processus centralisé qui garantisse une coordination efficace des procédures dans le cadre d'une coopération nationale et internationale. Les escroqueries de type « coup du neveu » relèvent également d'une approche en série par des bandes criminelles organisées au niveau international. En définitive, la collecte de données (type d'escroquerie mise en œuvre, numéros de téléphone, pseudonymes, empreintes vocales) est un élément fondamental de la poursuite de cette catégorie d'infractions. Il est donc judicieux de compiler les caractéristiques de référencement spécifiques des escrocs au « coup du neveu » en Suisse dans une base de données centralisée.

Infractions routières, violence domestique, gestion des menaces : Lors d'un contrôle de véhicule, les collaborateurs qui n'ont pas accès à POLAP n'obtiennent que des renseignements incomplets sur la personne à contrôler. Cette situation peut être illustrée par le cas d'un conducteur dont le permis de conduire a déjà été retiré plusieurs fois (dans un laps de temps relativement court) dans un canton X et qui conduit ensuite dans un canton Y où il est contrôlé pour la première fois. La police établira certes un rapport sur la conduite malgré un retrait de permis, mais elle ne confisquera pas la voiture en tant que moyen d'infraction, car cela ne se fait pas lors d'une première infraction. Toutefois, si la police a accès aux antécédents via POLAP, les mesures de coercition prises à l'encontre du prévenu dans un tel cas seront assurément plus sévères. Il sera justifié de saisir le véhicule et l'on pourra éventuellement demander une détention provisoire au motif du danger de réitération.

Les affaires de violence domestique, lorsqu'elles sont de faible gravité, n'aboutissent pas à la comparution du prévenu devant le procureur. En revanche, si les policiers disposaient dès le départ de l'accès à tous les dossiers préexistants du ou des prévenus dans les différents cantons, une remise serait possible même dans les cas se situant à la limite de la légalité (voie de fait oui/non/pas claire ou intensité de la menace pas claire).

Il en va de même dans les cas où seul un risque de passage à l'acte est rapporté. Par exemple, un individu dans un train régional se met à clamer que dans une semaine, toute la gare X explosera et qu'il y aura de nombreux morts et blessés. Dans une telle situation, aucune infraction n'a été commise, car aucune victime n'a pu déposer plainte pour menaces, mais le procureur doit décider, sur la base de ce seul incident, s'il convient de placer le prévenu en détention provisoire pour une expertise ou d'y faire procéder de manière ambulatoire, c'est-à-dire en liberté, par un spécialiste. Il est extrêmement difficile et risqué d'évaluer correctement les prévenus dans le court laps de temps d'un interrogatoire en détention. En revanche, si l'on disposait, dans de tels cas, d'indications sur des comportements similaires

dans d'autres cantons, voire sur des condamnations, cela faciliterait grandement la prise de décision en faveur ou à l'encontre d'une demande de détention provisoire.

3. POLAP

Responsabilités

La CCPCS constate que les structures techniques et juridiques de la plate-forme de recherche policière POLAP sont désormais plus claires. Concernant l'exploitation et le traitement des données dans POLAP, fedpol est défini comme responsable au sens de la LPD et comme exploitant. POLAP est exploité à l'intention des autorités de police des cantons et de la Confédération, le CSI-DFJP étant chargé de l'exploitation technique.

Compte tenu de ce qui précède, les tâches et les responsabilités de TIP en ce qui concerne POLAP peuvent être allégées. Il convient de réviser et de simplifier le texte du concordat à cet égard. Dans le cadre du projet, l'accent est mis sur la création des bases juridiques nécessaires pour que les données policières puissent être consultées et rendues accessibles de manière automatisée via une plate-forme de recherche.

Base légale

À l'échelon fédéral, les bases juridiques seront créées dans le cadre de la révision de la LSIP, qui devrait entrer en vigueur en 2026 selon le calendrier actuel.

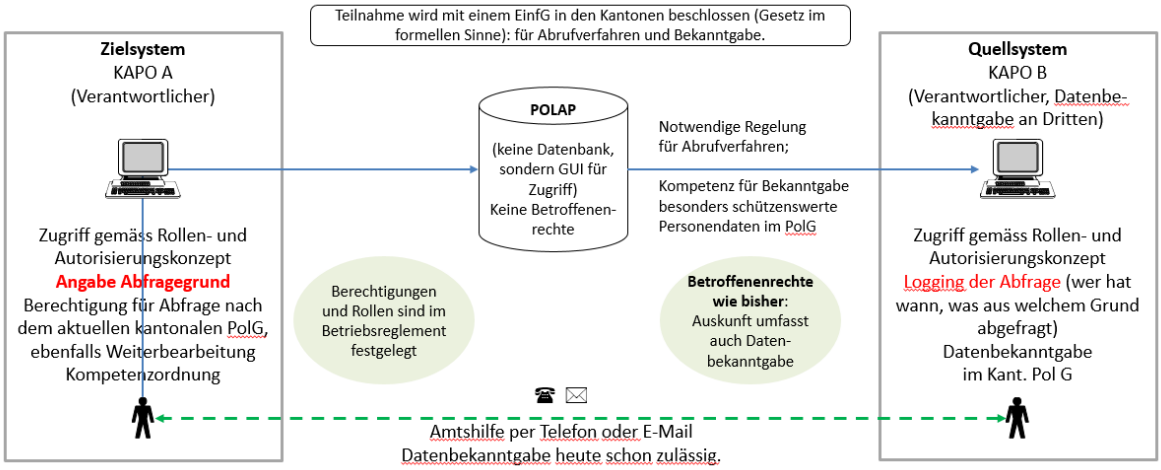
Sur le plan cantonal, la CCPCS constate que les bases juridiques existantes, dans les lois sur la police, permettent déjà aux autorités de police de la plupart des cantons d'échanger des données avec les autorités de police d'autres cantons et de les leur communiquer. Actuellement, cela se fait encore parfois au moyen de l'assistance administrative par téléphone ou par e-mail. POLAP ne vise pas à conférer de nouvelles compétences policières aux autorités de police, mais seulement à régler la procédure d'appel. Les échanges de données, qui ont déjà lieu aujourd'hui par des moyens physiques et analogiques, se feront désormais par le biais d'une procédure d'appel automatisée. Cela permettra de rendre les bases de données de police interopérables, ce qui est indispensable pour un travail de police moderne en Suisse.

Étant donné que diverses lois cantonales sur la police contiennent déjà des dispositions relatives à l'échange de données de police et à la procédure d'appel, il est intéressant d'analyser et de comparer les bases légales actuelles dans les différents cantons et les révisions en cours. La CCPCS espère ainsi déterminer dans quelle mesure les lois sur la police en vigueur ou leurs révisions imminentes offrent déjà une base légale appropriée pour que les autorités de police cantonales puissent interconnecter leurs systèmes sources à POLAP et fournir, par procédure d'appel, l'accès aux données qu'ils renferment.

Dans ce contexte, la relation et les conséquences de divergences entre les réglementations des lois cantonales sur la police et celles des concordats sont discutables. Cette question, entre autres, nécessite l'avis d'un expert.

Mode de fonctionnement

La CCPCS souligne que POLAP n'est pas une plate-forme d'interconnexion mais uniquement une plate-forme de recherche. Les informations qu'elle contient peuvent être consultées afin d'être « visualisées », POLAP offrant une vue standardisée des données exploitables conformément au rôle attribué (par ex. tâches judiciaires, de sécurité, de police administrative etc.) et au contexte choisi (par ex. contrôle à la frontière extérieure de l'espace Schengen, contrôle de personnes, contrôle de la circulation, autorisation de port d'arme etc.). Les données restent stockées exclusivement dans les systèmes sources.
La plate-forme de recherche policière POLAP peut être représentée schématiquement comme suit :



En tant que plate-forme de recherche policière, POLAP n'est pas une base de données, mais uniquement un moyen de visualiser des données dans des systèmes sources cantonaux. Aucune nouvelle donnée sur les personnes concernées ne peut y être enregistrée ni aucune donnée préexistante à partir des systèmes sources consultés. POLAP ne consigne ni les requêtes des utilisateurs ni les réponses du système, l'enregistrement de telles activités s'effectuant dans les systèmes sources interrogés. Les systèmes sources connectés vérifient également si les conditions d'une requête sont remplies avant de fournir une vue standardisée des données disponibles.

Pour la CCPCS, la loi applicable à un système source doit logiquement être déterminée en fonction de la responsabilité à l'égard du système source. Il est donc pertinent de laisser la responsabilité du traitement des données et des droits des personnes concernées aux responsables des systèmes sources. Les demandes de renseignements et autres droits d'accès de personnes intéressées doivent être communiqués aux responsables des systèmes

sources. Ainsi, POLAP n'entraîne pas de changement fondamental dans les responsabilités en matière de protection des données.

Compétences en matière de police

Compte tenu de ce qui précède, la CCPCS conclut que la présente convention intercantonale ne crée pas, dans le cadre de POLAP, de nouvelles compétences en matière de police. La convention doit uniquement avoir pour but de réglementer dans un cadre juridique global la procédure d'appel intercantonale et l'accès aux données ainsi que les questions de protection des données qui y sont liées (responsabilité, surveillance, sécurité des données, droit de consulter les pièces) lorsque cela n'est pas déjà garanti par les lois cantonales sur la police.

4. Systèmes de base de données communs

Recommandation a été faite aux cantons de déléguer la compétence en matière d'adoption des ordonnances d'exploitation à leur représentation au sein de l'assemblée stratégique TIP (v. rapport explicatif, p. 15). Conformément à l'art. 6. al. 2 de la convention TIP, il s'agit des *directrices et directeurs cantonaux de justice et police*. Certains cantons estiment que la voie des ordonnances d'exploitation pour créer la base juridique de tels systèmes de bases de données communs est trop peu élevée dans la hiérarchie des normes pour justifier les atteintes aux droits fondamentaux qui en résultent. Suite à l'entrée en vigueur du concordat, le peuple et les parlements n'auraient ainsi que peu voire pas d'influence sur la matière réglementée, qui présente pourtant en de nombreux points une importance telle qu'elle devrait, en fait, être réglée dans une loi formelle. Compte tenu des prises de position déposées, les points énumérés à l'article 18 doivent impérativement être réglés par le législateur et non par voie d'ordonnance d'exploitation. Il ne serait donc pas suffisant de fonder un système de base de données commun sur une ordonnance d'exploitation et il conviendrait alors de conclure, au regard de chaque système de base de données commun, une nouvelle convention intercantonale réglant les points fondamentaux de l'article 18.

Pour être recevable, une délégation législative au législateur doit se rapporter à une matière précise et bien définie et sa portée doit être clairement limitée. Dans la conception de la convention intercantonale, la CCPCS s'est efforcée de répondre à ces exigences, telles que formulées par le Tribunal fédéral dans l'arrêt 1C_39/2021 du 29 novembre 2022. La matière à réglementer – l'échange de données de police – a été décrite dans le projet de la manière la plus précise possible. Parallèlement, une attention particulière a été accordée à l'octroi d'une certaine marge de manœuvre aux autorités de police cantonales afin qu'elles puissent recourir à de nouvelles technologies et mettre en place d'autres systèmes d'information à des fins policières sans porter atteinte aux principes de l'État de droit.

Les nombreuses réactions critiques concernant la voie des ordonnances d'exploitation incitent la CCPCS à soumettre la conception correspondante à une analyse approfondie sous l'angle des droits fondamentaux et de la protection des données. Notons toutefois dès à présent que les ordonnances d'exploitation, en tant qu'actes normatifs cantonaux au sens

de l'art. 82 let. b LTF, peuvent faire l'objet d'un contrôle abstrait des normes, de la même manière que si elles étaient adoptées par l'ensemble du gouvernement de chaque canton.

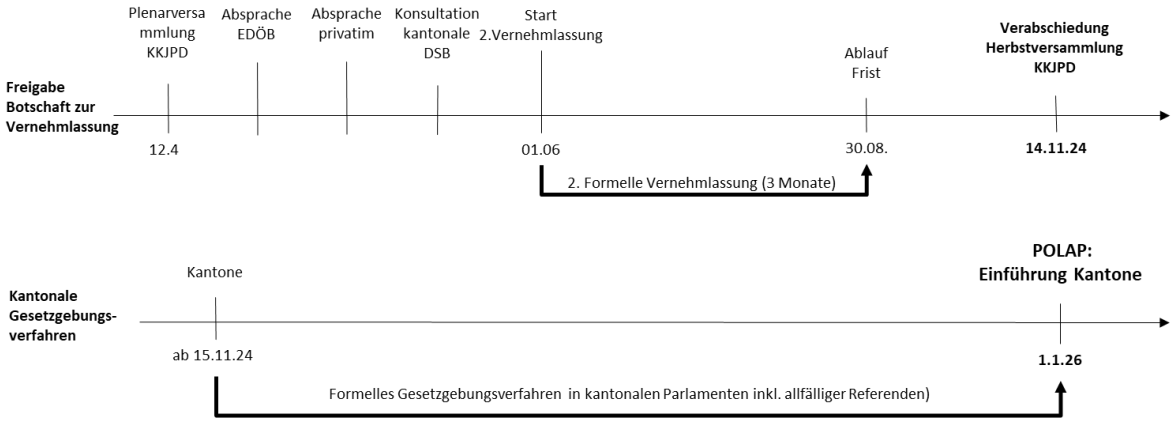
Dans un cadre plus large, les nombreux commentaires sur ce sujet soulèvent à nouveau la question des types de systèmes d'information qui doivent et peuvent être mis en place dans le cadre de cette convention (voir ci-après).

5. Suite de la procédure

Les commentaires des participants seront pris en compte et le texte du concordat révisé. Le projet reste axé sur un concordat régissant les plates-formes de recherche telles que POLAP et les systèmes de bases de données communs. Les éléments suivants seront notamment ajustés :

a) Ajustement de la structure de gouvernance du fait de la responsabilité de fedpol en tant qu'exploitant de POLAP et des nouvelles bases juridiques créées à cet effet dans la LSIP révisée.
b) Révision des catalogues d'infractions (en s'inspirant notamment des catalogues d'infractions figurant dans diverses lois fédérales).
c) Précision des systèmes déjà existants dans un nouvel alinéa (p. ex. transfert des concordats ViCLAS et PICAR avec un degré de précision analogue).
d) Concertation des exigences en matière de protection des données avec le PFPDT et Privatim. Participation de tous les services cantonaux de protection des données dans le cadre d'une réunion de consultation.

Il est prévu que le concordat soit adopté lors de l'assemblée plénière de la CCDJP du 14 novembre 2024, de sorte que la procédure de ratification puisse ensuite être lancée dans les cantons et que le lancement opérationnel de POLAP soit possible au début de 2026 (parallèlement à la révision de la LSIP). Le calendrier ajusté se présente comme suit :



Pour assurer que le projet bénéficie d'un large soutien auprès des cantons et des services intéressés, une deuxième procédure de consultation formelle sera organisée à la suite de la révision.