Audit de l'efficacité de la lutte contre la cybercriminalité
Office fédéral de la police

L'essentiel en bref

La criminalité numérique a des limites floues, des initiateurs incernables et souvent une dimension internationale. C'est un défi pour les autorités de poursuite pénale. Dans neuf cas sur dix, ces crimes relèvent de la compétence cantonale. Toutefois, l'Office fédéral de la police (fedpol) est essentiel dans cette lutte : comme office central et point de contact international, il apporte son aide aux polices des cantons. De plus, fedpol soutient le Ministère public de la Confédération (MPC) dans ses procédures de cybercrminalité complexe de compétence fédérale.

Le Contrôle fédéral des finances (CDF) a audité l'efficacité de la lutte contre la cybercriminalité chez fedpol. Il s'est rendu en Argovie, à Berne, dans le canton de Vaud, au Tessin et à Zoug ainsi qu'au MPC pour saisir l'environnement dans lequel fedpol évolue et la perception de ses partenaires. Les services de la Police judiciaire fédérale (PJF) – de sa division « IT Forensique & CyberCrime » (IFC) et de sa division « Criminalité économique » – sont appréciés par les cantons et le MPC. La lutte contre la pédocriminalité en ligne fait l'objet de clarifications entre les cantons et la Confédération. Le CDF identifie pourtant des pistes pour améliorer l'efficacité du suivi des affaires de la PJF, ses capacités d'analyse et sa coopération avec le MPC.

Adéquation des ressources chez fedpol et prestations jugées bonnes par les cantons

L'analyse d'un échantillon de dossiers personnels de l'IFC note une adéquation entre les compétences des employés et leurs tâches, même si des différences existent selon les fonctions. Le CDF voit un risque de démotivation chez les collaborateurs de l'IFC arrivés il y a peu et/ou avec des formations pointues en raison d'une progression salariale à l'ancienneté.

Les cantons vus par le CDF apprécient les prestations de l'IFC et son aide dans la coopération internationale. Faute de ressources, ces cantons identifient un besoin d'analyse de la cybercriminalité que fedpol pourrait développer à l'avenir. De plus, l'IFC trie aussi les annonces d'images interdites émises par ses partenaires – tel le National Center for Missing and Exploited Children – et les dénonce aux cantons. Pour le CDF et en application du cadre légal actuel, fedpol devrait améliorer le suivi de ces dénonciations auprès de ses partenaires cantonaux.

Collaboration et divergences avec le MPC, centralisation opportune des achats sur le plan fédéral

Avec fedpol, la sous-division Cyber du MPC mène des procédures de cybercriminalité complexes. Elle collabore sans difficulté majeure avec la PJF. Mais, le MPC et fedpol divergent sur la création d'un « cyber-commissariat » à la PJF, comme correspondant à la sous-division Cyber du MPC. Pour plus d'efficacité, ces autorités se sont réorganisées depuis dix ans et ont fait correspondre leurs structures (« effet miroir »). Or, ce n'est plus le cas avec la création de la sous-division Cyber au MPC fin 2019. A cette occasion, la communication entre ces autorités n'a pas non plus été optimale. Le CDF recommande à fedpol d'analyser les avantages et les inconvénients d'un « cyber-commissariat » à la PJF ou de toute autre solution pour assurer la disponibilité des ressources aux procédures pénales « cyber » du MPC d'ici juillet 2021.

Les entités fédérales – dont fedpol et le MPC – et les cantons dépensent plusieurs millions de francs par an en prestations forensiques IT auprès d'une seule société. Celle-ci réalise près de

80 % de son chiffre d'affaires avec le secteur public. Le CDF recommande à fedpol d'établir un centre de compétences, notamment forensiques, pour l'administration fédérale, et ainsi centraliser les besoins pour apporter une réponse économe et efficace dans ce domaine.

Environnement applicatif et traitement numérique des dossiers à renforcer en priorité

A l'IFC et à la PJF, le traitement numérique des données d'enquête n'est pas sans risques. La direction de fedpol a identifié cela début 2019. La situation devrait être améliorée via le programme « Ermittlungssystem » (ErmSys) avec une échéance ambitieuse en 2022. Le CDF recommande à fedpol de rendre prioritaire le programme ErmSys pour assurer un cadre de travail adéquat, sûr, assurant la traçabilité des informations pour les partenaires fédéraux et cantonaux de la PJF et donnant un support de travail efficace à ses équipes.

Sans outils performants et automatisés de pilotage, la PJF s'expose à un risque de conduite insuffisamment structurée des dossiers, limitant sa marge de manœuvre et l'anticipation des problèmes. Ces difficultés s'illustrent dans l'analyse d'environ 170 dossiers de *phishing* (hameçonnage de données). Sollicitée par le MPC en 2017, cette analyse a pris fin en octobre 2020. Le MPC attend encore la livraison des rapports de police. A l'avenir, la PJF prévoit la création d'un monitoring moderne intégré dans les améliorations envisagées par fedpol. Le CDF recommande à fedpol de renforcer les outils de pilotage des activités de la PJF grâce un monitoring (cockpit et indicateurs) pour la gestion des dossiers, y compris le suivi des dénonciations de fedpol aux cantons (images interdites).

Clarifications bienvenues dans la lutte contre la pédocriminalité numérique

Fin 2019, le Parlement a octroyé quatre postes à fedpol pour la cyber-pédocriminalité. Les documents reçus par le CDF montrent une traçabilité partielle lors de la création de ces postes, dont deux hors PJF. Ils ne permettent pas de dire si fedpol a respecté ou non la volonté du Parlement. Le CDF lui recommande d'examiner et de justifier l'allocation des postes afin que la décision du Parlement et les besoins exprimés par les cantons puissent être satisfaits.

La pédocriminalité numérique est de compétence cantonale. Depuis 2001, fedpol réalise toutefois des recherches actives contre cette criminalité au profit des cantons. Ici, le CDF a constaté un arrêt durant neuf mois en 2018 des enquêtes sous couverture contre les cyber-pédophiles. Dès le 1er janvier 2021, ces recherches actives iront désormais aux cantons selon une convention entre la Conférence des directrices et directeurs des départements cantonaux de justice et police et la Conférence des Commandants des Polices Cantonales de Suisse. La mise en œuvre incombe aux cantons dont les ressources pour relever ce défi se construisent. Pour le CDF, cette clarification du travail entre fedpol et les cantons est opportune.

Des indicateurs de performance pour la Stratégie nationale de protection contre les cyberrisques

Le CDF a audité le volet pénal de la Stratégie nationale de protection contre les cyberrisques (SNPC II) et la mise en œuvre des mesures relatives. Le Centre national pour la cybersécurité (NCSC) coordonne ces activités et effectue un contrôle de gestion stratégique. Il admet que des risques en matière pénale ne sont pas entièrement couverts. Ces risques font cependant l'objet d'un processus d'appréciation pour évaluer de nouvelles mesures à prendre.

Pour lutter contre la cybercriminalité, les mesures de la SNPC II à appliquer ont un caractère général et leurs calendriers mériteraient d'être précisés. Le NCSC ne dispose pas d'un monitoring critique de leur mise en œuvre. Pour une future SNPC III, le CDF recommande d'élaborer un système d'indicateurs de performance afin d'évaluer la réalisation des objectifs à atteindre pour chaque mesure.