Criminologie, Forensique, et Sécurité

Les innovations technologiques en contexte d'enquête policière

Une revue des enjeux et problématiques relatifs à la formation policière

Technological Innovations in the Context of Police Investigations

A Review of Issues and Challenges Regarding Police Training

Maxime Bérubé

Volume 2, numéro 3, 2024

Devenir policier

URI : https://id.erudit.org/iderudit/1117851ar
DOI : https://doi.org/10.26034/la.cfs.2024.4705

Aller au sommaire du numéro

Éditeur(s)

Association internationale des criminologues de langue française (AICLF)

ISSN

2813-6098 (numérique)

Découvrir la revue

Citer cet article

Bérubé, M. (2024). Les innovations technologiques en contexte d'enquête policière : une revue des enjeux et problématiques relatifs à la formation policière. *Criminologie, Forensique, et Sécurité*, *2*(3), 1–10. https://doi.org/10.26034/la.cfs.2024.4705

Résumé de l'article

Les sociétés contemporaines se caractérisent par de constantes transformations et évolutions technologiques et les forces de sécuritépublique n'échappent pas à ces changements. Les enquêteurs policiers, notamment, doivent porter de plus en plus d'attention aux technologies numériques dans le cadre de leur fonction afin de répondre le plus efficacement aux besoins en matière de criminalité technologique. Pour cette raison, de nouvelles formations sont mises en place au Québec et d'autres sont revues afin de mieux outiller les enquêteurs policiers à l'égard des nouvelles technologies. Dans cet article, des réflexions sont exposées afin de mieux comprendre le contexte de formation des enquêteurs policiers québécois. Tout d'abord, différents enjeux des technologies en enquête sont examinés en portant un regard critique sur le contexte québécois et en s'appuyant sur des concepts développés dans le champ des études sur la prise de décision. Ensuite, un portrait des différents types de formations actuellement disponibles et pertinents pour les enquêteurs policiers du Québec est dressé. Enfin, une série d'enjeux relatifs à la formation et au contexte opérationnel est expliquée de manière à permettre, en conclusion, une réflexion visant à améliorer l'off re de formation des policiers.

Criminologie, Forensique et Sécurité

www.revue-cfs.net | ISSN : 2813-6098

Organe officiel de l'association internationale des criminologues de langue française (AICLF)

Article régulier

Criminologie, Forensique et Sécurité

2024 | 2 (3) : 4705

https://doi.org/10.26034/la.cfs.2024.4705

Les innovations technologiques en contexte d'enquête policière : une revue des enjeux et problématiques relatifs à la formation policière.

Maxime Bérubé[1]

[1] Département de biochimie, chimie, physique et science forensique, Université du Québec à Trois-Rivières.
Contact : maxime.berube2@uqtr.ca

Résumé

Les sociétés contemporaines se caractérisent par de constantes transformations et évolutions technologiques et les forces de sécurité publique n'échappent pas à ces changements. Les enquêteurs policiers, notamment, doivent porter de plus en plus d'attention aux technologies numériques dans le cadre de leur fonction afin de répondre le plus efficacement aux besoins en matière de criminalité technologique. Pour cette raison, de nouvelles formations sont mises en place au Québec et d'autres sont revues afin de mieux outiller les enquêteurs policiers à l'égard des nouvelles technologies. Dans cet article, des réflexions sont exposées afin de mieux comprendre le contexte de formation des enquêteurs policiers québécois. Tout d'abord, différents enjeux des technologies en enquête sont examinés en portant un regard critique sur le contexte québécois et en s'appuyant sur des concepts développés dans le champ des études sur la prise de décision. Ensuite, un portrait des différents types de formations actuellement disponibles et pertinents pour les enquêteurs policiers du Québec est dressé. Enfin, une série d'enjeux relatifs à la formation et au contexte opérationnel est expliquée de manière à permettre, en conclusion, une réflexion visant à améliorer l'offre de formation des policiers.

Mots clés

Enquête policière, formation, trace numérique, cyberenquête, informatique judiciaire, science forensique numérique

Technological Innovations in the Context of Police Investigations: A Review of Issues and Challenges Regarding Police Training.

Abstract

Contemporary societies are marked by constant technological transformations, and public security forces are not immune to these changes. Police investigators, in particular, must increasingly focus on digital technologies within their roles to effectively address the growing demands related to technological crime. For this reason, new training programs are being implemented in Quebec, and others are being revised to better equip police investigators with respect to emerging technologies. In this article, reflections are presented to enhance understanding of the training context for Quebecois police investigators. Firstly, various issues related to technology in investigations are examined, critically assessing the Quebecois context and drawing on concepts developed in the field of decision-making studies. Subsequently, a comprehensive overview of the different types of currently available and relevant training for Quebecois police investigators is provided. Finally, a series of issues related to training and operational context is explained to facilitate, in conclusion, a reflection aimed at improving police training offerings.

Keywords

Police investigation, training, digital trace, cyber investigation, digital forensics, digital forensic science

Citation : Bérubé, M. (2024) Les innovations technologiques en contexte d'enquête policière : une revue des enjeux et problématiques relatifs à la formation policière. *Criminologie, Forensique et Sécurité*, 2 (3) : 4705.

Introduction

Au Québec, comme c'est le cas dans bien des pays du monde, la cybercriminalité est en constante augmentation, menaçant la sécurité de nos citoyens, de nos entreprises et de nos institutions publiques. La cyberintimidation, le partage non consensuel d'images intimes, le leurre d'enfants, les attaques informatiques, le vol d'identité, la fraude en ligne et plusieurs autres formes d'activités malveillantes sur Internet sont devenus monnaie courante, ceci sans compter les enjeux à venir dans la foulée de l'avènement du métavers et de l'intelligence artificielle et dont les impacts sont à prévoir au cours des prochaines années. Il est donc essentiel de mettre en œuvre des moyens rapides, efficaces et surtout à la fine pointe des avancées numériques et technologiques afin de fournir aux policiers les connaissances et les compétences nécessaires pour faire face à ces nouvelles formes de criminalité (Baraz et Montasari, 2023).

La panoplie de traces numériques générées par l'utilisation de ces technologies ouvre de vastes horizons pour les forces de l'ordre. Cependant, les avancées technologiques s'accompagnent d'un double défi : l'utilisation croissante des technologies par les criminels et l'adaptation complète des pratiques policières afin de pouvoir exploiter pleinement les traces numériques produites lors d'activités criminelles. En cette période particulièrement affectée par le manque de ressources et de formation en matière de criminalité technologique et de cybercriminalité, l'évolution rapide des technologies accentue la pression sur les acteurs du milieu, de même que sur l'offre de formation devant être mise à leur disposition. En effet, leur expertise est très spécialisée et elle doit être constamment mise à jour (Harkin , 2018). De plus, on constate que les études scientifiques s'étant penchées sur la question proposent différents enjeux devant être pris en compte, soit l'augmentation de la charge de travail des unités spécialisées, le manque de ressources, les contraintes opérationnelles et le degré de formation insuffisant (Delle Donne et Fortin, 2020; Harkin , 2018; Neiva , 2023).

Dans le cadre de cet article, nous proposons des réflexions approfondies visant à offrir une meilleure compréhension du contexte de formation dans lequel évoluent les enquêteurs policiers québécois et des enjeux qui s'y rattachent. Ces réflexions découlent de connaissances acquises dans le cadre de différents projets de recherche portant sur l'investigation numérique, ainsi que d'expériences sur le développement de formations universitaires en enquête et policières. Pour initier cette exploration, nous examinons de manière critique ce contexte dans lequel les policiers évoluent, de façon à mettre en lumière les divers enjeux liés aux innovations technologiques auxquels ils doivent faire face. Cette analyse s'appuie sur des concepts issus du domaine des études sur la prise de décision, appliqués au champ de l'enquête policière. Par la suite, nous dressons un portrait détaillé des différentes formations actuellement disponibles, spécifiquement adaptées et pertinentes pour les enquêteurs policiers du Québec. En abordant ces différents cours et programmes, nous ne cherchons pas à fournir une liste exhaustive des formations disponible, mais plutôt à donner un aperçu des principales ressources éducatives disponibles pour ces professionnels, et ce, en ne se limitant qu'aux domaines de l'informatique judiciaire et de la cyberenquête. Enfin, nous examinons une série d'enjeux cruciaux liés à la formation et au contexte opérationnel des forces de l'ordre. Ultimement, l'objectif de ce travail et de proposer des pistes d'amélioration de l'offre de formation des policiers et de moderniser les pratiques d'administration de la justice.

Mise en contexte - Les technologies en enquête policière

Depuis déjà plusieurs années, la criminalité se caractérise par une intégration exponentielle de nouvelles technologies numériques. Tout comme la population générale, les délinquants utilisent de plus en plus fréquemment des appareils mobiles, portent sur eux des appareils connectés, ou encore contournent les usages conventionnels d'appareils numériques pour en tirer profit, créant ainsi de multiples traces numériques (Bérubé, 2022; Dupont et Whelan, 2021). Cette transformation de la criminalité englobe à la fois des infractions relevant de crimes traditionnels pour lesquels les technologies constituent un outil (vol, meurtre, extorsion, méfait, etc.), ainsi que des cybercrimes à proprement dits où la technologie est prise pour cible (piratage, rançongiciel, attaque de déni de service, utilisation non autorisée d'un ordinateur, etc.) (Casey, 2011; De la Hoz, 2021). Afin de lutter efficacement contre cette criminalité moderne, les policiers doivent être en mesure de bien comprendre le fonctionnement de ces technologies et d'utiliser du même coup des outils technologiques d'enquête de plus en plus complexes visant à permettre l'exploitation plus optimale de ces traces. Une trace, dans le domaine de la science forensique, est le vestige d'une activité, observable ultérieurement, pouvant servir d'indice à la reconstruction d'événements passés (Bérubé, 2022). Les traces numériques sont donc un incontournable dans les enquêtes modernes. Elles existent sous de multiples formes et peuvent également être exploitées de différentes manières (Jaquet-Chiffelle , 2018; Mousseau , 2022). Plus précisément, les techniques relatives à l'exploitation de ces traces en milieu policier se trouvent souvent distinguées sous deux types d'expertises distinctes : la cyberenquête et l'informatique judiciaire (Choi , 2022). Pour la première, on s'intéresse plus spécifiquement aux techniques permettant la recherche et la sauvegarde de traces numériques sur Internet, par exemple sur les plateformes de médias sociaux, les archives du web, les salles de clavardage, etc. Ce type de pratique inclut également les opérations d'infiltration virtuelle pouvant être conduite dans ces environnements, ce qui nécessite alors des techniques d'enquête plus avancées (Baraz et Montasari, 2023; Bérubé , 2020; Powell et Haynes, 2020). Quant à l'informatique judiciaire, l'intérêt porte plutôt sur les traces numériques emmagasinées sur des supports numériques pouvant être saisis et analysés, comme des ordinateurs, des téléphones mobiles, des objets connectés ou intelligents, etc. (Barral , 2022; Casey, 2011; Jaquet-Chiffelle, 2013; Thomas-Brans , 2022). Compte tenu de l'augmentation des traces pouvant être traitées par les enquêteurs, le nombre de demandes d'assistance, donc la charge de travail, aux unités policières spécialisées dans ces deux domaines est en constante augmentation. Ces unités se retrouvent de plus en plus surchargées, limitant leurs capacités à se spécialiser et suivre le rythme de cette évolution comme il se devrait, parfois même au point de compromettre leur capacité à répondre aux demandes dans un délai raisonnable (Harkin , 2018). Ainsi, cela crée des retards de plusieurs mois dans le traitement des dossiers d'enquête, ce qui s'avère hautement problématique dans un contexte où, comme c'est le cas au Canada depuis le jugement *R c. Jordan* en juillet 2016, le système judiciaire impose des délais maximaux entre le dépôt des accusations et la conclusion du procès[1].

[1] *R. c. Jordan*, [2016] 1 RCS 631, 2016 CSC 27 (CanLII), <http://canlii.ca/t/gsds4>

L'adaptation des enquêteurs à cette nouvelle réalité, qu'ils soient spécialistes des technologies ou non, requiert une revue approfondie des pratiques actuelles afin de bien cibler les déterminants pouvant avoir une incidence sur la prise de décision relative à ces adaptations. Déjà, la littérature scientifique propose différents enjeux qui caractérisent ce secteur d'activité (Anderson , 2015; Dekker , 2020; Delle Donne et Fortin, 2020; Faubert , 2021). Premièrement, les défis relatifs à la disponibilité des ressources mettent en évidence les difficultés d'acquisition d'une main-d'œuvre qualifiée dans le domaine des nouvelles technologies (Boddington, 2012; Reedy, 2020) et le manque d'encadrement des qualifications requises pour occuper ces professions de plus en plus complexes (Casey, 2019; Jaquet-Chiffelle , 2018). Les spécialistes de l'investigation numérique disposent de compétences variées et pluridisciplinaires, impliquant notamment des connaissances en enquête, en informatique, en droit et en éthique, ce qui fait en sorte que les profils varient selon les contextes criminels auxquels ils doivent faire face. Ceux-ci sont formés de manière très spécifique selon les tâches qu'ils doivent accomplir au quotidien et les besoins de leur organisation (Reedy, 2020). Malgré cette spécialisation, Casey (2019) soutient tout de même que des lacunes importantes persistent dans le secteur public quant aux connaissances et aux capacités en investigation numérique. Il suggère que ces lacunes découlent d'un manque de ressources publiques, contrairement aux institutions privées qui détiendraient le monopole du développement grâce à leurs plus grandes capacités financières. Parallèlement à ce constat, l'état des connaissances actuelles montre également que le manque de ressources techniques dans les milieux policiers découle de diverses contraintes dans la gestion et la fluidité du partage des connaissances, entre autres, en ce qui a trait au déploiement et à l'adaptation aux techniques avancées dans le domaine des technologies numériques (Casey, 2019; Reedy, 2020).

Les organisations policières se caractérisent par des impératifs organisationnels et opérationnels ayant un impact sur la manière dont les décisions y sont prises. La culture organisationnelle policière, par exemple, souvent teintée par une méfiance envers autrui, une culture du secret et une résistance aux changements peut avoir des effets à différents niveaux sur la prise de décision et l'adaptation aux innovations en contexte d'enquête (Chan, 1996; Lingamneni, 1979; Monjardet, 1994). Celle-ci peut également nuire à l'établissement de collaborations multilatérales pouvant s'avérer judicieuses dans ce domaine complexe, notamment avec des institutions du secteur privé ou du milieu universitaire pouvant disposer de connaissances plus avancées sur certains aspects technologiques et mises à profit aux fins d'enquête (Casey, 2019; Faubert , 2021; Weisburd, 2005). Dans un même ordre d'idée, Casey (2019) souligne que contrairement à la culture générale des sciences, et plus particulièrement de la science forensique, « qui fonctionne en termes d'assurance qualité, de biais d'observation et d'évaluation de l'incertitude, la culture policière est plutôt enclin vers les résultats, la génération de pistes d'enquête et la résolution de cas » (traduction libre, p. 662). Dès lors, il est possible que des démarches soient entreprises sur la base de critères ne favorisant pas un traitement optimal des traces numériques en contexte d'enquête. Les contraintes opérationnelles entraînent aussi des limites en ce sens, alors que le temps alloué pour répondre aux exigences de l'enquête ou au cadre judiciaire, par exemple aux exigences du jugement *R c. Jordan* énoncé précédemment, ne tient pas pleinement compte de la lourdeur attribuable à la quantité massive de données à traiter dans la plupart des dossiers d'enquête actuels (Harkin , 2018). De plus, depuis plus d'une décennie, les études portant sur le sujet suggèrent que très peu d'enquêtes criminelles n'impliquent pas de traces numériques et que les tribunaux leur accordent de plus en plus d'importance dans les décisions qui sont rendues (Atkinson, 2014; Boddington , 2008; Carrier et Spafford, 2003; Casey, 2011).

Dans un même ordre d'idée, le contexte juridique dans lequel les traces numériques sont employées entraîne aussi son lot de difficultés. Afin d'être admissibles devant les tribunaux, les traces numériques exploitées en contexte d'enquête doivent être traitées avec beaucoup de rigueur (Boddington , 2008). Celles-ci ont d'ailleurs comme particularité de pouvoir être altérées et de présenter des incertitudes quant à leur authenticité et à leur interprétation (Bérubé, 2022; Bérubé , 2022). Ces incertitudes nécessitent un traitement minutieux de la trace et possiblement des expérimentations nécessitant des ressources dont les organisations policières ne disposent pas toujours (Casey, 2019). Si des éléments de preuve basés sur des traces numériques peuvent être admis à tort devant un tribunal, le manque de connaissance de la part des acteurs concernés par les démarches d'enquête ou judiciaires, notamment les praticiens du droit, peut également entraîner le rejet inapproprié de certaines d'entre elles (Boddington, 2012). Par ailleurs, Brown (2015) a démontré que le manque de connaissances spécialisées auprès des juges pouvait faire en sorte que des traces numériques plus complexes pouvaient être dévalorisées, alors que ces derniers tendent à accorder moins d'importance aux preuves qui leur sont moins tangibles. Les avocats, quant à eux, opteraient plus souvent pour les types de traces avec lesquels ils sont les plus familiers, ce qui risque également de limiter le potentiel de traces issues de technologies plus récentes. À cet égard, Akin (2011) soutient quant à lui que, pour les infractions de cybercriminalité par exemple, la complexité des traces numériques entraîne l'avortement de plusieurs dossiers d'enquête et de procès. En contexte juridique, lorsqu'un doute subsiste quant à l'attribution de la paternité d'une trace ou de l'interprétation de son contenu, sa valeur probante auprès d'un juge ou de jurés peut en être grandement affectée, voire complètement rejetée (Akester, 2004; Bérubé , 2022). Cela peut également être le cas lorsque l'intégrité ou la fiabilité des traces numériques ne peut être démontrée (Atkinson, 2014). Par exemple, dans une cause récente aux États-Unis, le juge a écarté les traces issues du service de géolocalisation de Google, sous prétexte que leur fiabilité n'était pas suffisamment reconnue par la communauté scientifique (Casey , 2020).

Qu'il soit attribuable à un manque de ressources, de connaissances ou de compétences, le risque d'erreur humaine, et plus particulièrement les erreurs d'interprétation, demeure un incontournable dans un domaine aussi dynamique que celui de l'investigation numérique (Casey, 2019). À cet égard, Reedy (2020) souligne que « le manque de compétence, tout comme une gestion organisationnelle privilégiant la rapidité à la qualité, peut conduire à la négligence et la mauvaise interprétation de certaines traces » (traduction libre, p.495). Maintenant que ces enjeux et problématiques sont bien définis, il s'avère que des formations initiales et continues constituent un atout important pour le personnel policier. L'importance des traces numériques doit être réellement prise en compte et intégrée pleinement dans les nouvelles formations qui sont développées, tout comme dans l'actualisation des formations existantes. Si l'on se concentre sur le contexte québécois et plus particulièrement sur les techniques d'enquête, il existe une variété importante de formations accessibles aux policiers pouvant leur permettre d'acquérir ou de parfaire les connaissances dans les domaines de la cyberenquête et de l'informatique judiciaire.

Portrait des formations offertes au Québec pour le développement des connaissances technologiques des enquêteurs policiers

Les policiers québécois souhaitant se doter de connaissances et de compétences en cyberenquête et en informatique judiciaires se voient proposer une offre de formation limitée, mais diversifiée, où ils ont la possibilité de suivre des cours spécifiquement conçus et dont l'accès est restreint aux forces de l'ordre, ou des formations offertes au grand public dispensées dans les cégeps et les universités[2]. Certaines formations privées sont également offertes aux enquêteurs policiers québécois, notamment par les fournisseurs de logiciels spécialisés en informatique judiciaire, mais puisque celles-ci se situent généralement hors du Québec et qu'elles sont très variées, elles ne seront pas abordées dans le cadre de cet article.

Les formations restreintes aux policiers

Au Québec, la Loi sur la police (RLRQ, c. P-13.1) impose à tout policier accédant à une fonction d'enquêteur de suivre et réussir le Programme de formation initiale en enquête policière (PFIEP) dispensée par l'École nationale de police du Québec (ENPQ)[3]. Cette formation de niveau universitaire issue d'une collaboration entre l'ENPQ, l'Université Laval, l'Université de Sherbrooke et l'Université du Québec à Trois-Rivières (UQTR), permet également l'accomplissement d'un Microprogramme de premier cycle de formation initiale en enquête chapeauté par l'UQTR[4]. Depuis sa refonte en 2023, un nouveau cours sur les technologies en contexte d'enquête policière a été ajouté à cette formation[5]. D'une durée de 45 heures et s'inscrivant dans une approche programme où d'autres enseignements technologiques sont aussi proposés, ce cours vise d'abord à familiariser les nouveaux enquêteurs à l'usage des nouvelles technologies, tant en contexte d'enquête que criminel. Il a également pour objectif de leur enseigner les bonnes pratiques d'utilisation sécuritaire de ces technologies dans le respect des politiques organisationnelles et du cadre légal en vigueur, de même qu'à développer leurs compétences pratiques pour l'utilisation de techniques et d'outils spécialisés. Pour ce faire, il a été conçu et il est diffusé conjointement par du personnel enseignant de l'UQTR et des experts policiers de la Sureté du Québec et du Service de police de la Ville de Montréal. De façon plus détaillée, cette formation couvre différentes thématiques. En premier lieu, il s'agit d'une introduction aux rudiments de la recherche sur Internet et la mise à niveau l'ensemble de participants sur les connaissances technologiques cruciales à détenir en contexte d'enquête policière. Parmi les connaissances devant être acquises dès le début de la formation figurent, entre autres, le fonctionnement des réseaux Internet et des adresses IP, la reconnaissance d'appareils et d'identifiants numériques, ainsi que les procédures légales de base comme la saisie de biens informatique ou les différents types de demandes légales pouvant être effectuées auprès des fournisseurs de service Internet, de télécommunications ou d'autres entreprises œuvrant dans le domaine des technologies numériques. Une fois les fondements des connaissances bien établis, les participants se voient mis à l'épreuve lors de simulations de perquisition d'appareils technologiques, en plus d'approfondir les connaissances vers des aspects plus avancés, notamment quant à la sauvegarde adéquate de traces numériques, les médias sociaux et diverses techniques pour la recherche en sources ouvertes. Ils y voient également plusieurs processus spécialisés d'informatique judiciaire, l'expertise d'ordinateur, d'appareils mobiles et d'autres technologies émergentes (drones, véhicules, objets connectés, etc.). Au terme de cette formation, les enquêteurs policiers se voient plus à même de faire face à des infractions de cybercriminalité, de même que des situations impliquant des cryptoactifs, l'intelligence artificielle, le dark web et des environnements de réalité virtuelle comme le métavers. Compte tenu de son caractère récent, obligatoire et transversal pour l'ensemble des enquêteurs policiers du Québec, qu'il s'agisse d'enquêteurs généraux ou dédiés à des unités spécialisées, cette formation au PFIEP est des plus centrale dans le développement des capacités et le perfectionnement des policiers du Québec à l'égard des nouvelles technologies. Néanmoins, ce n'est pas la seule formation dispensée par l'ENPQ à de telles fins.

Outre la formation initiale en enquête policière, l'ENPQ offre d'autres formations plus spécialisées, comme une formation de 40 heures dédiée précisément à l'infiltration virtuelle[6]. Cette formation, visant à mieux outiller les enquêteurs policiers affectés à une équipe d'enquête spécialisée en infiltration virtuelle, vise à développer les compétences pour la création de profils et le développement de stratégies d'infiltration dans l'espace numérique. Dans un autre ordre d'idée, un cours sur l'enquête sur la cybercriminalité est également offert aux policiers de patrouille-gendarmerie afin que ceux-ci puissent mieux comprendre la nature et les rouages de ce type d'enquête[7]. Autrement, des enseignements technologiques sont dispensés dans le cadre de formation nécessitant une approche plus particulière des traces numériques, comme c'est le cas par exemple pour les formations sur les crimes économiques, les crimes à caractère sexuel, la récupération d'actifs criminels, etc.

Les principales organisations policières québécoises, soit la Sureté du Québec et le Service de police de la Ville de Montréal, disposent quant à elle de formations développées ponctuellement en interne et visant à combler certains manques à travers la communauté policière, en plus de diminuer le nombre de demandes d'assistance adressées aux équipes spécialisées. À ce titre, la Sureté du Québec a par exemple initié, en collaboration avec l'ENPQ, une courte formation d'une heure pour les superviseurs de relève en patrouille-gendarmerie. Dans le cadre de cette formation, on y décrit les principaux éléments essentiels à l'identification d'éléments technologiques à récupérer sur les lieux d'une infraction, selon les différents types d'infractions. Par la même occasion, ces derniers sont aussi sensibilisés à la volatilité des traces numériques, qui fait en sorte que si les éléments essentiels d'identification ne sont pas prélevés dans les plus brefs délais, ceux-ci peuvent être perdus à jamais. Ils y apprennent également toute l'importance de la sécurisation de ces traces une fois prélevées adéquatement. Pour en citer un autre exemple, la Sureté du Québec offre sur une base annuelle une formation d'actualisation aux policiers affectés

[2] Plusieurs formations énumérées dans cette section ont été répertoriées dans une base de données construite par le Réseau intégré sur la cybersécurité (SERENE-RISC - https://www.serene-risc.ca/)

[3] https://www.enpq.qc.ca/policier/formation-enqueteur/cheminement/programme-de-formation-initiale-en-enquete-policiere

[4] https://oraprdnt.uqtr.uquebec.ca/pls/apex/f?p=106:10:2602419995519:::10:P10_CD_PGM:0998

[5] https://www.enpq.qc.ca/nos-formations/fiche?tx_annuaireenpq_annuairerecherche%5Bcours%5D=1298

[6] https://www.enpq.qc.ca/nos-formations/fiche?tx_annuaireenpq_annuairerecherche%5Bcours%5D=1801

[7] https://www.enpq.qc.ca/nos-formations/fiche?tx_annuaireenpq_annuairerecherche%5Bcours%5D=586

à l'intervention jeunesse et à la prévention lors de laquelle l'unité de cyberenquête est mise à contribution. Compte tenu de la nature de leur travail et de la clientèle qu'ils côtoient, il est primordial que ces derniers puissent être bien au fait des dernières innovations relatives aux technologies couramment utilisées par les jeunes d'aujourd'hui, notamment en lien avec leur utilisation des médias sociaux et applications de messageries numériques (De la Hoz, 2021).

Bien que le Collège canadien de police ne soit pas au Québec, cette institution d'enseignement dédié à la formation des forces policières propose également une gamme très vaste de formations spécialisées visant à renforcer les compétences des enquêteurs québécois confrontés aux défis complexes de l'informatique judiciaire et de la cyberenquête. Leur programme phare d'examinateur en informatique judiciaire, étalé sur 15 jours, s'adresse spécifiquement aux enquêteurs nécessitant des connaissances plus approfondies sur la fouille et les perquisitions informatiques[8]. On y enseigne des techniques avancées d'extraction de traces numériques, d'authentification et d'analyse des données numériques, tout en portant une attention particulière à assurer leur admissibilité devant le système de justice. D'autres formations spécialisées abordent des domaines spécifiques tels que l'analyse de traces numériques directement prélevées sur Internet, les stratégies et techniques pour mener des enquêtes de réseau, ainsi que les méthodes d'acquisition et d'analyse d'appareils mobiles, compte tenu des caractéristiques de sécurité de ces appareils qui sont en constante évolution. On y offre aussi des formations ciblées sur l'analyse des processus actifs, visant à acquérir des données plus volatiles comme la mémoire cache sur un ordinateur en fonction et sur les registres informatiques dont les données peuvent être exploitées aux fins d'enquête. Les formations avancées permettent le développement des capacités sur de nombreuses thématiques d'actualité, telles que les enquêtes approfondies sur la cybercriminalité, les techniques d'enquête en sources ouvertes et les enquêtes sur l'exploitation sexuelle des enfants sur Internet. Ces formations approfondies sont conçues pour fournir aux participants des compétences hautement spécialisées, indispensables pour mener des enquêtes efficaces dans ces domaines dynamiques et en constante évolution.

Les formations publiques accessibles et pertinentes aux enquêteurs policiers

En plus des formations spécifiquement dédiées et restreintes aux policiers, ces derniers ont également la possibilité de parfaire leurs connaissances en suivant des formations dispensées par des organisations civiles de niveau collégial et universitaire. Bien que ces formations ne soient pas conçues spécialement pour des enquêteurs policiers, mais plutôt un vaste éventail d'enquêteurs œuvrant dans différents types d'organisations, comme des banques, des entreprises, des firmes d'investigation ou d'autres services de réglementation, elles peuvent offrir des enseignements technologiques pertinents, notamment sur des aspects liés à des domaines connexes comme la cybersécurité ou la réponse aux incidents informatiques.

Au niveau collégial, il existe une gamme complète de formations spécialisées axées plus particulièrement sur la cyberenquête et la cybersécurité[9]. Plusieurs cours se concentrent sur divers aspects comme la compréhension des différentes normes et réglementations en vigueur dans les organisations et sur les enjeux liés à la cyberenquête et la sécurité informatique. Les participants y acquièrent une expertise pratique grâce à des projets concrets, des simulations, des études de cas, et l'utilisation d'outils spécialisés. Les formations incluent également des modules d'introduction pour permettre une immersion progressive dans le domaine de l'informatique.

Du côté des formations universitaires, autres que celles mentionnées précédemment et qui ne s'adressent qu'au personnel policier, différents certificats sont accessibles et pertinents pour les enquêteurs policiers. Une des principales universités ayant développé une expertise dans ce type de formation est Polytechnique Montréal où toute une panoplie de certificats[10] est offerte dans différents domaines pouvant être mobilisés à des fins d'investigation numérique. Ces formations couvrent divers aspects des réseaux informatiques, de la sécurité numérique, de la cybercriminalité et de la gestion des risques liés à la sécurité de l'information. Les participants peuvent y parfaire des connaissances sur les réseaux informatiques et se familiariser avec les principaux éléments matériels nécessaires au fonctionnement de ceux-ci. Les formations abordent également les aspects liés à l'adressage, les applications web, le transfert de fichiers et les vulnérabilités des services Internet. Des formations portent également sur la cybersécurité, abordant notamment la protection des applications Internet, le chiffrement, le contrôle d'accès, la cyberfraude, l'analyse de preuves numériques, la prévention des attaques, et l'enquête en matière de cybercriminalité. Les formations abordent également les aspects juridiques, éthiques et sociaux liés à la cybercriminalité, les enjeux de vie privée, les lois et réglementations, ainsi que la gestion des incidents de sécurité et la réponse à ceux-ci. Les participants explorent également les technologies émergentes telles que l'intelligence artificielle, l'Internet des objets et la cryptographie quantique, ainsi que les défis et les meilleures pratiques associés à ces évolutions. En résumé, ces formations offrent une approche permettant aux participants de mieux faire face aux défis relatifs à l'évolution constante de la sécurité informatique et de la cybercriminalité. De plus, ces formations permettent un service ayant l'avantage de pouvoir être mobilisé d'une manière « à la carte » où les participants ont la possibilité de choisir les cours qui sont les plus cohérents avec leurs besoins.

Dans un même ordre d'idée, d'autres universités offrent des certificats, comme le certificat en enquête et renseignement de l'Université de Montréal ou des formations continues, dans lesquels certains cours portent notamment sur la trace numérique, la cybercriminalité et la recherche d'information sur Internet[11]. Les participants y explorent les concepts du transfert de la trace numérique, l'utilisation d'appareils électroniques dans la commission d'infractions criminelles, pénales ou réglementaires, la préparation et la collecte d'information, la perquisition électronique et les processus judiciaires qui découlent de l'enquête. Sur le plan de la cybercriminalité, les participants sont entre autres formés au fonctionnement général d'Internet et aux principaux services existants dans cet environnement, comme les médias sociaux, puis sur les impacts sociaux de la cybercriminalité. Aux fins d'enquête, on leur enseigne les rouages

[8] https://www.cpc-ccp.gc.ca/programs-programmes/technological-technologique/cmpfor-infjud-fra.htm

[9] Voir par exemple : https://fc.cegepgarneau.ca/cyberenquete ou https://formationcontinuecegepsth.ca/cours/cyberenquete/

[10] https://www.polymtl.ca/programmes/cours

[11] https://admission.umontreal.ca/programmes/certificat-en-enquete-et-renseignement/

de la recherche en ligne à l'aide des moteurs de recherche Internet et les méthodes d'anonymisation des activités d'investigation. Ces formations, enrichies par des exercices pratiques, visent à doter les enquêteurs de compétences rudimentaires sur les technologies numériques essentielles à connaître pour mener à bien des activités d'enquête et de renseignement dans le domaine numérique. On constate, par la présentation de ces différents cours et programmes, qu'il existe tout un éventail de formations accessibles aux enquêteurs policiers québécois afin de parfaire leurs connaissances à l'égard des nouvelles technologies en contexte d'enquête. La diversité de celui-ci s'avère encore plus grande lorsque l'on y inclut également les formations accessibles à l'étranger, ou encore par le biais de formation en ligne.

Enjeux opérationnels et difficultés relatives à la formation policière

Dans l'objectif de contribuer à l'amélioration des formations développées à l'attention du personnel policier enquêteur, les sections qui suivent visent à mettre en lumière un certain nombre d'enjeux relatifs à ces formations qui en limitent les retombées, que ce soit en lien avec les formations elles-mêmes ou aux contextes opérationnels dans lesquels elles sont appelées à contribuer. Dans une perspective où les objectifs généraux sous-jacents de ces formations visent le développement transversal des capacités policières dans l'usage des technologies numériques en enquête et la réduction de la surcharge des unités spécialisées en cyberenquête et en informatique judiciaire, la simple mise à disposition de formations ne peut être suffisante et différents facteurs sont à considérer afin d'assurer les retombées souhaitées de ses formations. Dès lors, en s'appuyant sur les observations qualitatives effectuées, il a été possible de déterminer des limites quant à la cohérence et la complexité des formations, de même que l'adaptation nécessaire des acteurs impliqués, et ce, à l'intérieur d'environnements où les ressources sont variables.

La cohérence entre les besoins et les formations disponibles

D'abord, bien que des formations complémentaires sur une base volontaire soient toujours appréciables et demeurent une nécessité, il est souhaitable qu'un niveau suffisant de formation initiale soit prévu dans les formations obligatoires au personnel policier. Cette manière de procéder vient notamment limiter les effets pouvant découler d'un manque de ressources qu'il est possible d'attribuer à la formation continue pour les milieux policiers. Dans un contexte où les organisations policières doivent traditionnellement jongler avec des ressources financières restreintes (Casey, 2019), ces dernières ne disposent pas toujours des budgets suffisants pour former adéquatement l'ensemble de leur personnel sur cet aspect. De surcroit, celles-ci dépendent aussi généralement d'effectifs restreints. Cela fait en sorte que, lors de l'affectation de personnel policier à des formations, ceux-ci ne peuvent accomplir leurs tâches habituelles, notamment leur fonction d'enquêteur, ce qui risque de nuire ou ralentir les opérations s'il n'y a pas suffisamment de personnel pour les remplacer. Nonobstant ces effets, le besoin de formation continue demeure un incontournable dans le domaine des technologies et des incitatifs doivent être mis à dispositions des organisations et du personnel policier.

Néanmoins, au stade de la formation initiale, il est nécessaire de pouvoir assurer une uniformité de la matière enseignée et que celle-ci réponde au besoin de transmission des bonnes pratiques, tout en prenant en considération l'ensemble des normes légales applicables et des réalités policières. Pour ce faire et s'assurer que les enseignements sont bien ancrés dans les réalités du terrain, les formations mises en œuvre devraient nécessairement se faire par le biais d'une collaboration entre du personnel policier et du personnel enseignant, tant lors de la conception des formations que de leur diffusion. De cette façon, il est possible de tirer profit d'intervenants assurant le recours à de bonnes pratiques pédagogiques et à l'intégration des savoirs policiers dans un ensemble d'enseignement plus général. D'une part, cela permet notamment de bonifier la formation dispensée en y intégrant des concepts sociologiques et scientifiques, par exemple sur les biais d'interprétation de la trace numériques, qui permettent d'avoir un regard critique et externe sur les savoirs conventionnels policiers et les méthodes pédagogiques habituellement privilégiées dans ce milieu. D'autre part, la présence de personnel policier dans la formation est capitale afin de pallier le fait qu'en contexte d'enquête policière, la formation implique la transmission de connaissances et de techniques policières qui ne sont généralement pas bien connues par le grand public. Les policiers, notamment ceux issus des unités spécialisées en cyberenquête et en informatique judiciaire, sont les plus à même de connaître ces connaissances et techniques faisant l'objet de la formation, de même que les voies les plus optimales de formation pouvant permettre d'alléger les demandes d'assistance dirigées à l'endroit de leurs propres unités. Une telle collaboration s'avère donc des plus optimales et profitable. Néanmoins, bien que l'offre de formation que nous avons présentée semble considérable, peu d'entre elles répondent à l'ensemble de ces critères de cohérence et de disponibilité des ressources. Par conséquent, le constat actuel démontre qu'un retard persiste dans la formation des policiers et que l'offre de formations spécialisées dans les nouvelles technologies devrait être bonifiée.

La complexité des technologies numériques

S'il existe aujourd'hui un retard à combler dans le développement des capacités policières, celui-ci peut s'avérer d'autant plus difficile à rattraper en raison de la diversité de technologies impliquées dans les investigations numériques et devant être connues par les enquêteurs policiers (Bérubé, 2022). Alors que l'on constate une popularité grandissante des espaces de stockages infonuagiques, des objets connectés et des applications de communication numérique, par exemple, la quantité et la diversité des traces pouvant s'avérer profitables aux fins d'enquête augmentent de manière fulgurante. Nous ne sommes plus dans une ère où l'enquêteur policier n'a qu'à saisir et sécuriser l'ordinateur présent sur un lieu d'intérêt pour y trouver l'ensemble des traces numériques pouvant être pertinentes à son dossier. Il est de plus en plus fréquent que celui-ci doive plutôt faire un tri parmi une panoplie d'appareils technologiques afin de repérer ceux qui sont d'intérêt pour son enquête et qui sont les plus probables de contenir les données qu'il recherche. De plus, il doit être en mesure de reconnaître d'autres appareils sur les lieux qui pourraient lui apporter des informations pertinentes, ou des sources de données distantes. Ces appareils peuvent prendre plusieurs formes, ce qui peut les rendre parfois difficiles à reconnaître, et les possibilités que ces appareils peuvent apporter dans le cadre d'une enquête sont aussi de plus en plus variées.

Cette diversité des dispositifs numériques implique le recours à différents appareils et logiciels afin d'être en mesure de traiter les données adéquatement et de manière à respecter les règles appli-

cables et en assurer la validité devant les tribunaux (Neiva , 2023). Elle génère une fragmentation du travail basée sur les spécificités des compétences des examinateurs qui se pencheront sur certains éléments de preuve plutôt que l'ensemble de l'enquête (Verma et Bansal, 2019). De plus, la majorité des technologies impliquées dans les enquêtes sont protégées par des droits de propriétaires, ce qui n'en permet pas l'accès à tous les acteurs impliqués dans les processus d'enquête (Novak, 2020). Cette dernière particularité fait également en sorte que les outils utilisés constituent des sortes de « boites noires » dont le code source et le fonctionnement interne sont généralement inconnus (Bhat , 2021). D'ailleurs, il n'est pas rare de voir différents logiciels produire des résultats divergents (Casey, 2019), ou encore pour lesquels il est impossible de déterminer les facteurs d'erreur associés aux résultats qu'ils produisent (Bhat , 2021; Garfinkel, 2010, 2013). Néanmoins, l'augmentation constante du volume de traces numériques à traiter en contexte d'enquête rend inévitable le recours à ces logiciels, voire même à plus d'un logiciel à la fois pour l'analyse d'un même corpus de données (Bérubé, 2022).

La modification constante des environnements numériques.

L'adaptabilité, en contexte technologique, est indispensable. Autant dans les pratiques d'enquête policière que de la formation, il est primordial que les différents acteurs de ces milieux soient en mesure de suivre l'évolution des innovations et des environnements en changements constants. De nouvelles décisions judiciaires sont rendues quotidiennement et les pratiques policières évoluent au rythme de ces nouvelles contraintes et des avancées technologiques. Par conséquent, les procédures applicables à la gestion et la manipulation des appareils numériques sont constamment reformulées, ce qui nécessite une adaptation des formations et des pratiques à une fréquence très élevée. Nécessairement, comme ce type de formation propose des enseignements qui se traduisent directement dans le contexte professionnel des participants, il se doit d'être à la fine pointe des avancées technologiques qui évoluent, dans ce domaine, à un rythme effréné et qui peuvent aussi être influencées par divers événements sociaux, politiques, législatifs, etc. Pour en citer un exemple, récent, plusieurs politiques organisationnelles et gouvernementales canadiennes ont interdit l'utilisation du réseau social TikTok, alors qu'il était largement utilisé auparavant et nécessaire à connaître en contexte d'enquête[12]. Du jour au lendemain, les usages, voire même la pertinence pour certains types d'enquête, de cette application dans le contexte policier ont radicalement changé. Une partie de la population a cessé de l'utiliser et plusieurs organisations y ont bloqué l'accès, tandis qu'une autre partie s'est mise à l'utiliser davantage en raison notamment de sa marginalité. Il devient alors nécessaire de revoir le contenu des enseignements en fonction de l'évolution de son usage et de celui d'autres applications connexes vers lesquelles plusieurs utilisateurs se sont tournés.

Afin de pallier ce problème, les organisations policières produisent ponctuellement du matériel didactique, comme des documents d'information et de référence ou des capsules vidéo, mais ce matériel est le plus souvent développé en silo, sans réelle collaboration entre les organisations. De plus, ce matériel peine à rejoindre le personnel policier sur le terrain, souvent par manque de communication en interne. D'importantes ressources doivent être dédiées pour la production de ce type de matériel, alors que le résultat n'est souvent qu'éphémère, puisqu'il se retrouve généralement dépassé dans un délai très court. Afin de capitaliser sur ces efforts et de limiter les ressources nécessaires en ce sens, il serait préférable d'établir des processus de formation initiale et continue, ou encore de partage optimal de l'information, de manière conjointe et qui peut rejoindre l'ensemble de la communauté policière.

Dans un autre ordre d'idée, s'il était d'usage de cloisonner les champs de la cyberenquête et de l'informatique judiciaire, tant à des fins opérationnelles que de formations, l'évolution des technologies fait en sorte que ce fractionnement disciplinaire traditionnellement bien établi se complexifie également. On constate notamment que, puisque les appareils numériques tendent à emmagasiner la majeure partie de leurs données dans des espaces infonuagiques où la sécurité est assurée par des procédés de chiffrement des données, de nouvelles techniques sont développées dans le secteur de l'informatique judiciaire afin d'accéder et de sauvegarder directement ces traces par le biais d'appareils lors de leur saisie. Une sorte de nexus entre le monde de la cyberenquête et de l'informatique judiciaire prend alors forme et la distinction entre ces deux approches s'amenuise (Bérubé, 2023). L'appareil saisi ne constitue plus uniquement l'endroit où les traces se trouvent. Il devient également un intermédiaire pour l'accès à des données distantes ou le déploiement d'autres démarches en cyberenquête. Les innovations récentes tendent en effet de plus en plus vers une interopérabilité des technologies, tout en diminuant à la fois les distinctions entre le monde réel et virtuel. C'est le cas par exemple avec l'utilisation des cryptomonnaies et du métavers qui impliquera de plus en plus une intégration technologique de réalités diverses (impliquant la réalité virtuelle et réalité augmentée), où les distinctions entre celles-ci seront de plus en plus ténues (Interpol, 2024).

La variation des ressources et le degré d'autonomie

Dans le domaine de l'investigation numérique, les ressources matérielles sont un incontournable pour assurer un certain degré d'efficacité et d'efficience dans le traitement des traces qui y sont exploitées. Les traces numériques, comme nous l'avons déjà évoqué, sont caractérisées par diverses particularités qui complexifient le travail des enquêteurs (Bérubé, 2022). En effet, celles-ci se retrouvent en quantité souvent beaucoup trop importante pour être traitée manuellement. Elles sont aussi très diversifiées et nécessitent d'être triées et catégorisées, tant au moment de leur saisie, de leur acquisition, que de leur analyse ou de leur divulgation pour la Cour (Horsman, 2022). Toutefois, les différents niveaux de service qu'offrent les organisations policières au Québec font en sorte que ceux-ci ne disposent pas des mêmes ressources humaines, matérielles et logicielles. Au Québec, il existe six niveaux de service policier à travers lesquels sont partagées les organisations policières (Cusson et Diotte, 2007; Mousseau , 2019). Ces niveaux de service, établis en fonction de la quantité de population desservie, dictent les infractions tombant sous leur juridiction et les ressources dont elle dispose. Ce ne sont donc pas toutes les organisations qui disposent d'unités dédiées à la cyberenquête et à l'informatique judiciaire. Par exemple, ce ne sont que les 6 services de police de niveau 3 et plus qui sont dotés d'une unité d'informatique judiciaire, minimalement

[12] Voir par exemple https://ici.radio-canada.ca/nouvelle/1959383/application-tik-tok-appareils-intelligents-interdiction-federale-canada-chine

pour l'extraction de banques de données informatiques[13]. Dans les autres cas ou les situations plus complexes, les enquêteurs bénéficient du soutien des unités de la Sureté du Québec qui a pour mandat d'appuyer les corps policiers municipaux lorsque les événements qui surviennent dépassent leur niveau de responsabilité. Bien que cela permette de diminuer les ressources nécessaires à l'ensemble de la communauté policière au Québec, la facilité d'accès aux ressources de ces unités en est par le fait même affectée. À des fins de formations, il est nécessaire de tenir compte de la réalité de chacun afin de proposer une majorité d'enseignements qui ont un potentiel d'applicabilité dans la plupart des différents milieux de pratique. Cela s'avère particulièrement difficile lorsque les participants évoluent dans des contextes de criminalité différents, qu'ils n'ont pas accès aux mêmes outils et qu'ils ne disposent pas de la même aisance à l'égard des nouvelles technologies. Malgré ces réalités distinctes, une ligne directrice de bonnes pratiques doit être établie pour la formation et les enquêteurs doivent par la suite l'appliquer selon leurs contraintes respectives.

La complexité, en termes de formation, revient à devoir identifier cette ligne directrice qui doit être maintenue afin d'assurer un degré de connaissances et de compétences optimales pour l'ensemble des enquêteurs policiers. Il est nécessaire de statuer sur le niveau d'autonomie suffisant dont ces derniers doivent faire preuve pour être en mesure de mener à bien la majeure partie des tâches qu'ils ont à accomplir au quotidien, avec les ressources dont ils disposent, sans toutefois qu'ils soient contraints à s'aventurer dans des tâches plus complexes qui nécessiteraient l'intervention de spécialistes dans un domaine particulier. Au-delà d'un certain seuil de complexité, évidemment variable en fonction des technologies, le risque d'erreur pouvant compromettre l'intégrité ou l'interprétation adéquate d'une trace augmente. Au risque de nuire à l'enquête, l'enquêteur doit plutôt faire appel au soutien de l'unité spécialisée dans le domaine en question. Or, ce seuil n'est pas le même pour tous les enquêteurs, puisque ceux-ci n'ont pas accès aux mêmes ressources, en plus de ne pas disposer du même degré d'aisance avec les nouvelles technologies. En effet, un autre enjeu devant être pris en compte dans la conception et l'offre de formation relève du degré de familiarité du personnel avec les nouvelles technologies. Étant donné que tous n'amorcent pas ces formations avec des niveaux de connaissances et de compétences similaires, une certaine mise à niveau s'avère nécessaire avant de pouvoir penser atteindre un degré d'aisance uniforme avec les technologies et le niveau d'autonomie souhaité. Enfin, comme c'est le cas pour la mise à jour constante du matériel pédagogique en fonction de l'évolution des technologies, le niveau d'autonomie souhaité variera lui aussi naturellement dans le temps à mesure que la prépondérance des technologies augmentera dans les dossiers d'enquête policière.

Conclusion

En cette ère où la saine et efficiente gestion des traces numériques prend de plus en plus d'importance dans les enquêtes criminelles, il est primordial que les enquêteurs policiers y soient bien formés. L'objectif de cet article visait à dresser un portrait de la situation actuelle des enjeux de la formation des enquêteurs québécois en ce qui a trait au développement de leurs capacités technologiques, de manière à proposer des pistes de réflexion d'améliorations plus générales des formations développées à l'endroit des policiers. Considérant la spécificité du contexte québécois et les différences significatives entre les systèmes d'organisation du travail policier d'une province canadienne et d'un pays à l'autre (Dupont, 2007), ce papier se concentre délibérément sur les considérations locales du Québec. Bien que des comparaisons avec d'autres provinces ou pays ne soient pas présentées, il est important de noter que les enjeux de formation policière, notamment le besoin de formations spécialisées, sont des préoccupations partagées à l'échelle internationale (Dupont, 2021; Holt , 2019). Plus précisément, nous avons pu constater, dans les paragraphes qui précèdent, qu'entre autres la disponibilité des ressources, humaines et matérielles, la variété de spécialisation possible dans le domaine des technologies numériques, les impératifs organisationnels, la culture policière, le cadre juridique, les spécificités de la trace numérique et la complexité de son interprétation, sont des facteurs clés à prendre en considération dans l'élaboration de formations policières. Bien qu'il ait été démontré que ceux-ci disposent de tout un éventail de formations accessibles, celles-ci ne sont pas forcément conçues à leur attention et ne prennent pas forcément en compte l'ensemble de ces facteurs. Cela fait en sorte que peu des formations disponibles proposent réellement des apprentissages adaptés au milieu policier.

À la lumière des réflexions présentées sur les enjeux opérationnels et les difficultés relatives à la formation, il appert que pour optimiser les formations en enquête policière liée aux nouvelles technologies, il est essentiel de prioriser l'intégration de compétences technologiques dès la formation initiale, en favorisant une collaboration étroite entre le personnel policier et les enseignants. Les contenus de formation doivent couvrir divers aspects technologiques, de la reconnaissance d'appareils à la compréhension des sujets les plus complexes, tout en intégrant ces apprentissages dans leur contexte social afin de favoriser la bonne interprétation des traces numériques recueillies. Il est crucial d'assurer une adaptabilité constante des formations pour suivre l'évolution rapide des technologies et des environnements numériques, avec une définition claire du niveau d'autonomie souhaité pour les enquêteurs. La mise à niveau préalable et la collaboration entre les domaines de la cyberenquête et de l'informatique judiciaire sont également recommandées pour garantir une uniformité des compétences et une réponse adéquate aux défis opérationnels spécifiques à chaque contexte policier.

Une fois que les recommandations précédentes sont mises en œuvre pour la formation initiale, la formation continue devrait se concentrer sur le maintien et le renforcement des compétences acquises. Les programmes de formation continue devraient être constamment adaptés aux évolutions continues des technologies numériques et des environnements légaux. Il est impératif d'intégrer des mises à jour régulières pour refléter les nouvelles décisions judiciaires, les avancées technologiques et les changements dans les comportements des utilisateurs. Il est également primordial pour les enquêteurs de pouvoir maintenir la main sur les compétences acquises qu'ils n'ont pas l'occasion de mettre en pratique régulièrement. Dans cette perspective, la formation continue constitue un atout pour assurer le maintien de ces compétences.

Enfin, pour avoir un impact encore plus important dans la lutte contre la criminalité, il s'avère également essentiel d'intégrer des formations adaptées aux nouvelles technologies pour l'ensemble des premiers répondants en sécurité publique pouvant contribuer aux enquêtes policières, particulièrement le personnel de patrouille-gendarmerie, de même qu'à l'ensemble des acteurs du système judiciaire. Ces formations devraient inclure une sensibi-

[13] Gatineau, Laval, Longueuil, Québec, Montréal et la Sûreté du Québec.

lisation générale aux enjeux technologiques, des enseignements sur les éléments essentiels d'information à connaître pour assurer la collecte et l'exploitation des traces numériques, ainsi que des formations continues sur les tendances et technologies émergentes afin que ces derniers demeurent bien au fait des particularités de celles-ci et des impacts de ces évolutions sur la criminalité. De cette façon, le système de justice québécois sera plus à même d'offrir une réponse adéquate et optimale aux infractions modernes, de leurs signalements jusqu'aux procès qui en découleront.

Références

Akester, P. (2004). Internet law: authenticity of works: authorship and authenticity in cyberspace. *Computer Law & Security Review*, 20(6), 436-444.

Akin, T. (2011). Cybercrime: Response, investigation, and prosecution. Dans R. Herold et M. K. Rogers (dir.), *Encyclopedia of Information Assurance* (p. 749-753). CRC Press.

Anderson, M., Lewis, K. et Dedehayir, O. (2015). Diffusion of innovation in the public sector: Twitter adoption by municipal police departments in the U.S. Dans. PICMET '15: Management of the Technology Age, Portland, OR, USA.

Atkinson, J. S. (2014). Proof is not binary: The pace and complexity of computer systems and the challenges digital evidence poses to the legal system. *Birkbeck Law Review*, 2(2), 245-261.

Baraz, A. et Montasari, R. (2023). Law enforcement and the policing of cyberspace. Dans R. Montasari, V. Carpenter et A. J. Masys (dir.), *Digital transformation in policing: The promise, perils and solutions* (p. 59-83). Springer.

Barral, H., Jaloyan, G.-A., Thomas-Brans, F., Regnery, M., Géraud-Stewart, R., Heckmann, T., Souvignet, T. et Naccache, D. (2022). A forensic analysis of the Google Home: Repairing compressed data without error correction. *Forensic Science International: Digital Investigation*, 42-43.

Bérubé, M. (2023, 12 janvier). *La scène de crime numérique : Incertitudes*. Communication dans le cadre d'un atelier de recherche du Centre de recherche de l'École des officiers de la Gendarmerie nationale (CREOGN), Paris, France.

Bérubé, M. (2022). Les traces numériques au service de la justice. Dans V. Denault (dir.), *Enquêtes, procès et justice : La science au service de la pratique* (vol. 2, p. 279-300). Éditions Yvon Blais.

Bérubé, M., Allard, S. et Denault, V. (2022). Ensuring the probative value of web searches as digital evidence. *Canadian Criminal Law Review*, *26*(2), 167-173.

Bérubé, M., Tang, T.-U., Fortin, F., Ozalp, S., Williams, M. L. et Burnap, P. (2020). Social media forensics applied to assessment of post–critical incident social reaction: The case of the 2017 Manchester Arena terrorist attack. *Forensic Science International*, *313*.

Bhat, W. A., AlZahrani, A. et Wani, M. A. (2021). Can computer forensic tools be trusted in digital investigations? *Science & Justice*, *61*(2), 198-203.

Boddington, R. (2012). A case study of the challenges of cyber forensics analysis of digital evidence in a child pornography trial. Dans. Annual ADFSL Conference on Digital Forensics, Security and Law.

Boddington, R., Hobbs, V. et Mann, G. (2008). Digital evidence for legal argument. Dans. Australian Digital Forensics Conference, Perth, Australia.

Brown, C. S. (2015). Investigating and prosecuting cybercrime: forensic dependencies and barriers to justice. *International Journal of Cyber Criminology*, *9*(1), 55-119.

Carrier, B. et Spafford, E. H. (2003). Getting physical with the digital investigation process. *International Journal of Digital Evidence*, *2*, 1-20.

Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers and the Internet*. Elsevier Academic Press.

Casey, E. (2019). The chequered past and risky future of digital forensics. *Australian Journal of Forensic Science*, *51*(6), 649-664.

Casey, E., Jaquet-Chiffelle, D.-O., Spichiger, H., Ryser, E. et Souvignet, T. (2020). Structuring the evaluation of location-related mobile device evidence. *Forensic Science International*, *32*.

Chan, J. (1996). Changing police culture. *The British Journal of Criminology*, *36*(1), 109-134.

Choi, K.-S., Back, S. et Toro-Alvarez, M. M. (2022). *Digital Forensics and Cyber Investigation.* Cognella Inc.

Cusson, M. et Diotte, M.-È. (2007). Les organismes de sécurité intérieure au Québec: Une classification. Dans M. Cusson, B. Dupont et F. Lemieux (dir.), *Traité de sécurité intérieure* (p. 89-97). Éditions Hurtubise.

De la Hoz, G. T. (2021). New trends in online crime using social networking sites and apps against children and adolescents: Police-based longitudinal research. *International Journal of Cyber Criminology*, *15*(1), 31-49.

Dekker, R., van den Brink, P. et Meijer, A. (2020). Social media adoption in the police: Barriers and strategies. *Government Information Quarterly*, *37*(2), 1-9.

Delle Donne, J. et Fortin, F. (2020). Innovation and policing: Factors influencing the adoption of social medias by members of Quebec police organizations. *Policing: A Journal of Policy and Practice*, *14*(3), 726-739.

Dupont, B. (2007). Police communautaire et de résolution des problèmes. Dans M. Cusson, B. Dupont et F. Lemieux (dir.), *Traité de sécurité intérieure* (p. 98-114). HMH Hurtubise.

Dupont, B. (2021). La police et la prévention de la cybercriminalité. Dans B. Dupont, A. Amicelle, R. Boivin, F. Fortin et S. Tanner (dir.), *L'avenir du travail policier* (p. 49-88). Presses de l'Université de Montréal.

Dupont, B. et Whelan, C. (2021). Enhancing relationships between criminology and cybersecurity. *Journal of Criminology*, *54*(1), 76-92.

Faubert, C., Décary-Hétu, D., Malm, A., Ratcliffe, J. H. et Dupont, B. (2021). Law enforcement and disruption of offline and online activities: A review of contemporary challenges. Dans M. W. Kranenbarg et R. Leukfeldt (dir.), *Crime in context: The human factor in victimization, offending and policing* (p. 351-370). Springer.

Harkin, D., Whelan, C. et Chang, L. (2018). The challenges facing specialist police cyber-crime units: an empirical analysis. *Police Practice and Research*, *19*(6), 519-536.

Holt, T., Lee, J. R., Liggett, R., Holt, K. M. et Bossler, A. (2019). Examining perceptions of online harassment among constables in England and Whales. *International Journal of Cybersecurity Intelligence & Cybercrime*, 2(1), 24-39.

Horsman, G. (2022). Triaging digital device content at-scene : Formalising the decision-making process. *Science & Justice*, 62(1), 86-93.

Interpol. (2024). *Metaverse: A law enforcement perspective - Use cases, crime, forensics, investigation, and gouvernance*. Interpol.

Jaquet-Chiffelle, D.-O. (2013). *Introduction à la criminalistique numérique*. Écoles des sciences criminelles de l'Université de Lausanne. https://serval.unil.ch/resource/serval:BIB_DFE9D125DECA.P001/REF

Jaquet-Chiffelle, D.-O., Casey, E., Pollitt, M. et Gladyshev, P. (2018). *A framework for harmonizing Forensic science practices and digital/multimedia evidence*. https://serval.unil.ch/resource/serval:BIB_32FB580596A3.P001/REF

Lingamneni, J. R. (1979). Resistance to change in police organization : The diffusion paradigm. *Criminal Justice Review*, 4(2), 17-26.

Monjardet, D. (1994). La culture professionnelle des policiers. *Revue française de sociologie*, 35(3), 393-411.

Mousseau, V., Baechler, S. et Crispino, F. (2019). Management of crime scene units by Quebec police senior managers: Insight on forensic knowledge and understanding of key stakeholders. *Science & Justice*, 59(5), 524-532.

Mousseau, V., Bérubé, M., Dumont, P.-L. et Crispino, F. (2022). Science forensique et criminologie : Vers une co-construction diversifiée des savoirs sur le phénomène criminel et sa régulation. *Revue internationale de criminologie et de police technique et scientifique*, 3(22), 1-13.

Neiva, L., Machado, H. et Silva, S. (2023). The views about Big Data among professionals of police forces: A scoping review of empirical studies. *International Journal of Police Science & Management*, 25(2), 208-220.

Novak, M. (2020). Digital Evidence in Criminal Cases Before the U.S. Courts of Appeal: Trends & Issues for Consideration. *The Journal of Digital Forensics, Security and Law*, 14(4), 1-42.

Powell, A. et Haynes, C. (2020). Social media data in digital forensics investigations. Dans X. Zhang et K.-K. R. Choo (dir.), *Digital Forensic Education* (p. 281-303). Springer Cham.

Reedy, P. (2020). Interpol review of digital evidence 2016-2019. *Forensic Science International*, 2, 489-520.

Thomas-Brans, F., Heckmann, T., Markantonakis, K. et Sauveron, D. (2022). New diagnostic forensic protocol for damaged secure digital memory cards. *IEEE Access*, 10, 33742-33757.

Verma, R. et Bansal, P. (2019). Scope of managing knowledge in digital forensics. Dans. International Conference on Sustainable Computing in Science, Technology & Management (SUSCOM), Jaipur, India.

Weisburd, D. L. (2005). The diffusion of computerized crime mapping in policing: Linking research and practice. *Police Practice and Research*, 6(5), 419-434.