International Journal of Management, IT & Engineering
Vol. 11 Issue 07, July 2021
ISSN: 2249-0558 Impact Factor: 7.119
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

L'INFORMATIQUE ET LA POLICE ; *défi et opportunité pour la Police Nationale Congolaise.*

Par NGOY WA NGOY MUTUALE Léon

Professeur Associé à l'Institut Supérieur de Lubumbashi (ISC-LUBUMBASHI)

Abstract

A crime is no longer necessarily locally directed and has become multifaceted. Thus, can it be organized thousands of kilometers away using computer networks located in different territories.

The low cost of technology and the unregulated growth of the Web have created lucrative avenues for criminals, making citizens and organizations vulnerable, not only through direct physical contact, but through cybercrime; a fact that further complicates the work of law enforcement! The Congolese police force by virtue of its original missions should no longer be satisfied with its traditional methods and techniques to accomplish its missions, it must appropriate New Information and Communication Technologies to take advantage of them in relation to its work. Naturally, certain forms of crime had as obligatory channels, the communication by word of mouth to elaborate their operational strategies and the physical presence at the scene of the crime; but today, mobile telephony, the Internet bypass all these traditional methods making the accomplishment of crimes and their refinement even more efficient.

Citizen expectations have also been stimulated by the dominant accountability movement and discussion of causes that receive media attention. Add to this an unwavering taste for dramatic series in which all crimes are solved. This context puts pressure on the Police to further increase the work of investigating, discovering and punishing crimes on the basis of a law outdated by the new forms of offences.

In this logic, Arielle Chemla declares that "Indeed, in the case of "ordinary" crime, police forces should have sufficient means and techniques to deal with cybercrime; otherwise, the specificities of cybercrime should give rise to a specialization of police forces. Faced with the obstacles to the criminal response that cyberspace poses,

law enforcement has had to adapt". Lawless zone", "legal void", or "anomic virtual platform": the application of criminal law in the digital world is sometimes so weak that the literature does not hesitate to compare cyberspace to a world without law because of the difficulty of applying digital criminal law. Indeed, repression comes up against two major obstacles limiting the scope of the fundamentals of criminal law: French territoriality in cyberspace under construction and the identification of anonymous offenders.

As a result, public opinion is increasingly expecting the police to broaden their field of intervention, change their methods of action and adapt their repression to the requalification of offences arising from the law. As a reminder, the population could call on the police for a quarrel between neighbors, for a rabid dog, to arrest burglars of property in a building or on a public road. Citizens wanted everything on demand in real time, including a physical police presence anywhere. In addition, tight budgets, poorly controlled and poorly managed geographic spaces no longer allow for a police officer to be posted on every street corner, to react in real time, especially given the urgent need for a police force. It is therefore imperative to consider cybercrime, which is taking on proportions that are not sufficiently controlled.

Keyword :

- Police
- Computer science
- Prevention
- Automation
- Monitoring
- Remote monitoring
- Protection
- Security
- Crime
- Cybercrime

Résumé :

Uncrimen'estplusnécessairementdirigédefaçonlocale et il est devenu multiforme. Ainsi,peut-il êtreorganiséàdesmilliers de kilomètres à l'aide de réseaux informatiques situés dans différentsterritoires.

Les faibles coûts de la technologie et la croissance non réglementée du Web ont créé des voies lucratives pour les criminels, rendant les citoyens et les organisations vulnérables, non seulement par contact physique directe, mais par la cybercriminalité ; fait qui complique davantage le travail de la police ! La police congolaise de par ses missions originelles ne devrait plus se contenter de ses traditionnelles méthodes et techniques pour accomplir ses missions, elle doit s'approprier de Nouvelles Technologies de l'Information et de la Communication pour en tirer profit par rapport à son travail.Naturellement, certaines formes des crimes avaient comme voies obligées, la communication de bouche à l'oreille pour élaborer leurs stratégies opérationnelles et la présence physique sur le lieu du crime ; mais aujourd'hui, la téléphonie mobile, l'Internet font contourner toutes ces traditionnelles méthodes rendant encore plus efficace l'accomplissement des crimes et leur raffinement.

Les attentes des citoyens ont également été stimulées par le mouvement dominant en matièrederesponsabilisationetladiscussionentourantlescausesquiretiennentl'attentiondes médias.Ajoutonslegoûtindéfectiblepourlessériesdramatiquesdanslesquellestouslescrimes sont résolus. Ce contexte exerce une pression sur la Police pour alourdir davantage le travail d'investigation, de découverte et de répression des crimes sur base d'une loi dépassée par les nouvelles formes d'infractions.

Dans cette logique, Arielle Chemla déclare qu' « En effet, dans le cas d'une criminalité « ordinaire », les forces de police devraient avoir les moyens et techniques suffisantes pour faire face à la cybercriminalité ; dans le cas contraire, les spécificités de la cybercriminalité devraient donner lieu à une spécialisation des forces de police. Face aux obstacles à la réponse pénale que le cyberespace oppose, la répression a dû s'adapter.« Zone de non-droit », « vide juridique », ou encore « plateforme virtuelle anomique » : l'application du droit pénal dans le monde numérique est parfois si faible que la littérature n'hésite pas à comparer le cyber- espace à un monde sans droit du fait de la difficulté de l'application du droit pénal du numérique. La répression se heurte en effet à

deux obstacles majeurs limitant la portée de fondamentaux du droit pénal : une territorialité française dans le cyberespace en construction et l'identification des délinquants anonymes »[*].

Par voie de conséquence, l'opinion publique s'attend de plus en plus à ce que la police élargisse son champ d'intervention, change ses méthodes d'action et adapte sa répression à la requalification des infractions en provenance de la loi. A titre de mémoire, la population pouvait faire appel aux policiers pour une querelle entre voisins, pour un chien enragé, pour arrêter les cambrioleurs des biens dans un bâtiment ou sur une voie publique. Les citoyens veulent tout obtenir sur demande en temps réel, y compris une présence physique de police en tout lieu. Par ailleurs, les budgets serrés, les espaces géographiques mal maitrisés et mal gérés ne permettent plus de poster un policier à chaque coin de rue, de réagir en temps réel, particulièrement en raison du besoin urgent de mettre en place un corps policier. A cela, il est impérieux de considérer la cybercriminalité qui prend des ampleurs non suffisamment maitrisées.

Mots clés :

- Police
- Informatique
- Prévention
- Automatisation
- Surveillance
- Télésurveillance
- Protection
- Sécurité
- Criminalité
- Cybercriminalité

Aujourd'hui, le corps policier se trouvedevant un véritable dilemme. Son rôle fondamental dans la société est resté le même en s'appuyant sur l'une des branches de la Police Nationale Congolaise, notamment, la Police Administrative qui se définit à partir d'une trilogie :

- La Sécurité publique : prévention des dommages aux personnes et aux biens.

[*] Chemla, A., « Réprimer les infractions numériques : une tâche lourde et lente », in *Sécurité globale2019/3 N° 19*, https://www.cairn.info/revue-securite-globale-2019-3-page-39.html, en ligne, le 9 février 2021.

- La tranquillité publique : prévention des perturbations de la rue, du tapage nocturne, etc.
- La salubrité publique : protection de la santé et de l'hygiène (Congolaise, 2010, p. 3).

La police doit veiller sur le respect de la loi et à la protection des biens et des personnes comme elle l'a toujours fait. Par ailleurs, son environnement d'intervention ne ressemble en rien à celui d'il y a 10, 15 à 20 ans. Or les différentes règles, lois et autres textes légaux datent parfois plus de ces années dans la mesure où les mentalités humaines, les types des crimes, les outils et méthodes évoluent et se complexifient perpétuellement.

Lalonguetraditiondel'attitudedu«travailaccompli»delapolices'esttraduiteparsaréacti on admirable à ce changement. Les policiers veulent faire tout ce qui est en leur pouvoir pour s'adapterettirerlemaximumdesressourcesafinderépondreauxbesoins.Cependant,lerythme du changement exige une nouvelle approche : l'utilisation des logiciels contre les pirates, les programmes malveillants et les diverses formes d'attaques (criminalités) bien appuyés par la télésurveillance.

Le corps policier du monde entier a réalisé que les ressources traditionnelles ont été exploitées au maximum,etqueseull'abandonde cemodèletraditionneldeservicesdepoliceréactifs–résoudre des crimes une fois qu'ils ont été commis – pour mettre l'accent sur un modèle proactif – le programme de prévention – leur permettra de s'attaquer directement à ces nouveauxdéfis.

De ce qui précède, à travers l'informatique, certaines Nouvelles Technologies de l'Information et de la Communication ainsi que des nouvelles perspectives ont été abordées comme moyens d'apport à la Police, en l'occurrence : les nouvelles perspectives, l'utilisation des logiciels et la télésurveillance.

I. DES NOUVELLESPERSPECTIVES

Un modèle proactif requiert un changement de processus et l'adoption d'une nouvelle technologie afin d'orienter le travail des policiers vers des tâches qui produisent de meilleurs résultats. Il peut s'appliquer à cinq secteurs principaux.

- **Une prévention éclairée**

Une approche plus systématique à l'égard de la cueilletteet del'analysededonnéesrévélantlestendancesdel'activitécriminelleentraîneruneutilisation plus efficace des ressources pour cibler le crime et leprévenir.

- **Lacollaborationentrelesorganismes**

Entravaillantenétroitecollaborationaveclesautres organismes, la police pourra appréhender les criminels plus rapidement, intervenir de concert lorsd'incidentsgravesettrouverdenouvellesméthodespourprotégerlesvictimespotentielles.

- **Le passage à la mobilité**

Les corpslorsqu'ils travaillent sur le terrain. L'utilisation généralisée des appareils mobiles personnels sécurisés peut répondre à ce besoin. Ces technologies mobiles réduiront également l'obligation pour les policiers de retourner à la station pour rédiger un compterendu.

- **Lasurveillancecitoyenne**

Lapolicedevramobiliserlescitoyensàl'aidedesréseaux sociaux et d'autres technologies afin de les inciter à assister la justice. Ils auront la possibilité de recueillir des preuves et de mettre un frein aux activitéscriminelles.

- **Laluttecontrelacybercriminalité**

Lapolicededemaindevraêtreprêteàs'attaquer directementàlacybercriminalitéenalertantlescitoyensdecomportementsoudesitesàéviter et en suivant de nouveaux comportements et criminels sur leWeb.

1. SURVEILLANCE DES RÉSEAUX SOCIAUX

Actuellement, la vitesse de la circulation des informations sur les réseaux sociaux est plus rapide que sur tout autre média dans le monde. L'observation des conversations sur les réseaux sociaux permet de déceler les signaux révélateursparmitoutlebruit,etd'anticiperainsilesproblèmes.Latechnologiepeutcontribuer à donner un sens à ce « bruit » social et à orienter la police en direction des risquespotentiels.

Les messages sur Twitter peuvent, par exemple, révéler les intentions violentes d'un groupe d'amateurs de football lors d'unmatch à l'étranger. La police pourrait alors réagir enmultipliant sa présence au site du match pour intercepter les agitateurs. Dans certains cas, la police n'aurait qu'à intervenir sur les mêmes médias sociaux pour calmer

les esprits en informant immédiatement la communauté virtuelle qu'elle exerce une surveillance. C'est, comme à titre illustratif, ce à quoi fait allusion André Clarinval : « Il y aurait *alors*, *peut*-être, moins de partant(e)s *pour* le djihad en Syrie. ... sur *sa page* Facebook le texte *d'un mail* islamophobe particulièrement haineux et ... la non moins cochonne Scarlett Johansson dans "*Match* Point". »[†]

Dans le cadre de la Police Nationale Congolaise, la présente pratique devrait même être instituée dans la loi et les règles de fonctionnement des tous les services de renseignements généraux afin de rendre la Police Administrative plus proactive plus qu'elle en est à ce jour, car peut-on observer, comme si elle était dépassée ou surprise par les évènements !

2. DÉFINIR LESPROFILS

Uneautreapproche, dans les services de Police très modernisés,consisteàanticiperlacriminalitéauseindescriminelsoudesréseaux decriminelsconnus.Enciblantunerégionouungroupedepersonnes,l'analytiqueseconcentre sur un groupe de données très précises décrivant leurs mouvements. L'activité criminelle antérieure d'un groupe ou d'une personne est analysée afin de prévoir de façon relativement exacte la suite des événements, selon les profils émergents. En fait, les données historiques constituent un système de prévision rapide del'activité.

C'est à ce niveau que les services de Police spécialisée tels que le Département de renseignements généraux, la police criminelle et la Police scientifique devraient disposer des bases des données conservant des informations et données relatives sur les diverses formes de criminalités habituellement connues et leurs auteurs ayant déjà été interpelés. Malheureusement, l'esprit de la routine aveugle plusieurs dans ce domaine pour ne plus capitaliser cet apport, non de moindre de l'informatique, dans les activités d'enquête, de recherche et d'investigation dévolues à ces Services.

3. LEÇONS EN PREVENTIONCIBLEE

Frantz Denat note que : « Mais le premier écueil ne vient pas des forces policières, quel que soit le système en place. Il réside dans un manque de courage politique, souvent doublé d'une absence de vision ou de projet à long terme. Dans le monde entier, en effet, alors qu'en termes de santé ce concept est universellement

[†]www.andre-clarinval.be › pages › journal, en ligne, le 8 février 2021

reconnu, parler de prévention en matière de criminalité semble être considéré comme une faiblesse institutionnelle ou structurelle »[‡]

Un organe policier régional du nord de l'Europe a analysé les données sur un groupede personnes libérées de prison et a noté qu'elles étaient plus susceptibles de récidiver au cours d'une période précise. La police les a surveillées de près pendant cette période à risque et a communiqué avec elles par l'entremise des services sociaux pour les empêcher derécidiver.

Au regard de ce qui précède, la Police Nationale congolaise a du pain sur la planche pour mener de telles actions afin de prévenir la criminalité tout aussi traditionnelle que celle apportée par les Nouvelles technologies de l'information et de la communication. Le manque de politique et compétence à ce sujet sont la vraie cause de cette difficulté que notre police rencontre. Théoriquement, ce terme est textuellement repris dans presque tous les documents qui réglementent la PNC. Le réalisme et l'opérationnalité de ce concept restent encore un mythe pour ne pas dire un mystère.

Les difficultés de mise en œuvre d'une telle perspective sont légion sur divers aspects commesur le plan partenariat, le plan technique, le plan interne amplifiés par le manque de vision politique cohérente. C'est l'idée que Frantz Denat partage avec nous en ces termes : « … ensuite, au sein de l'institution, l'action préventive n'est pas valorisée au-delà des discours : considération hiérarchique, avancements dans les grades, prestige de l'action, valorisation dans les médias, quantification tenant lieu d'évaluation… tout relève de la police répressive. Il faut évoquer aussi l'imaginaire de la population et des policiers eux-mêmes »[§].

Du reste, une telle démarche, à notre humble avis, devrait être mise en place sur trois principaux axes ;

1. Des interventions basées sur :

- Les programmes ciblant les enjeux scolaires et académiques.
- Les programmes ciblant les compétences personnelles et sociales.

2. De l'approche de l'évaluation basée sur :

[‡]**Frantz** Denat, « Prévention… Le rôle de la police », in *revue internationale d'éthique sociétale et gouvernementale*, vol. 4, n° 2 | 2002, https://journals.openedition.org/ethiquepublique/2201, en ligne, le 8 février 2021.

[§]**Frantz** Denat, *Op. Cit*, , https://journals.openedition.org/ethiquepublique/2201, en ligne, le 8 février 2021

- La réalisation des évaluations
- La synthèse des études d'évaluation aux fins du présent rapport
- Les limites ou insuffisances des études.

3. Des constatations portant aussi sur :

- Les connaissances et attitudes sur la Police, les délits et le système de justice
- Les facteurs de risques et de protection
- Les comportements liés à la criminalité.

En outre, pour en finir avec cette section, nous proposons ci-dessous le modèle canadien, programme novateur, celui des Programmes de prévention de la criminalité juvénile associée aux gangs[**]. Pour raisons illustrative et pratique ; nous présentons ce programme en intégralité car, dit-on, on n'invente pas la roue quand celle-ci existe !

Voici le programme de prévention de la criminalité juvénile associée aux gangs canadien tels que présentéspar l'**Institut canadien de formation**[††] **;**

LeBreaking the Cycle :

1. **Population cible:** Jeunes à risque de participer à des activités des gangs âgés de 15 à 26 ans

De plus, les jeunes qui participent à ce programme doivent :

- être impliqués présentement dans les gangs ou l'avoir été,
- être présentement sans emplois ou ne pas fréquenter l'école,
- s'engager à participer activement dans le projet et,
- s'engager face aux normes et aux accords du groupe.

Le programme Breaking the Cycle Youth Gang Exit and Ambassador Leadership (BTC) est administré par ICF - l'Institut canadien de formation. Le BTC est une stratégie complète qui vise les gangs de jeunes et qui visent à réduire les facteurs de risque chez les jeunes susceptibles d'entrer dans un gang ou qui en sont déjà membres.

2. Les principaux objectifs de BTC sont de :

- réduire l'appartenance aux gangs dans les collectivités ciblées;

[**] https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/prmsng-mdl-vlm2/index-fr.aspx#toc_5a, en ligne, le 8 février 2021

[††] Institut canadien de formation, John Sawdon, Directeur exécutif 50 Euston Ave Toronto, Ontario, Canada, M4J 3N3, http://www.cantraining.org/BTC/docs/Sawdon%20Evans%20CT%20Article.pdf, en ligne, le 8 février 2021.

- réduire les facteurs de risque tels que l'agressivité, la toxicomanie, le non emploi, les relations négative avec les pairs, qui contribuent à l'adhésion potentielle aux gangs;
- accroître le nombre de personnes sur le marché du travail parmi les participants;
- accroître le nombre de personnes engagées dans des activités prosociales parmi les participants.

3. Méthodologie

Les éléments clés de ce programme sont les suivants :

- de deux à trois semaines intensives de développement personnel. Cette phase se divise en deux programmes d'apprentissage, un pour les hommes et un pour les femmes, et les sujets abordent différentes thématiques, incluant par exemple, le sexisme et l'agression. Une emphase est également mise sur les habiletés de communication et les relations interpersonnelles.
- Une semaine de gestion des cas où des plans individuels sont développés. Les jeunes sont évalués afin de mesurer et de qualifier leur cheminement à travers le programme. À la fin de l'évaluation, des jeunes sont sélectionnés pour participer au programme *Youth Ambassador*.
- Le programme *Youth Ambassador Leadership and Employment*, est d'une durée de 28 semaines et se limite à deux groupes de 25 jeunes. Dans ce volet, les jeunes divisent leur temps entre leur cheminement personnel de croissance (développement et acquisition d'habiletés sociales, cognitives, comportementales et morales) et des activités de sensibilisation telles que la présentation d'exposés auprès des jeunes de leur âge dans les écoles, les familles, les groupes communautaires et également auprès des médias afin de sensibiliser les autres jeunes à risque et l'ensemble de la population aux dangers de s'affilier aux gangs.

4. Renseignements additionnels

Le programme Breaking the Cycle découle de l'expérience acquise par l'Institut canadien de formation sur les gangs lors de la mise en œuvre, vers la fin des années 1990, du projet intitulé “Beyond the Halls”. Ce projet avait été implanté dans quatre écoles secondaires du grand Toronto.

5. Évaluation

- Selon une évaluation du programme réalisée pour la période du 1e juillet 2003 et le 30 juin 2004 pour le compte de Ressources humaines et Développement des compétences Canada, le programme BTC, auquel 14 jeunes ont participé, a permis notamment :
    - De développer chez ces jeunes des habiletés d'employabilité aussi bien que d'acquérir une expérience et une confiance concernant la présentation d'exposé dans la collectivité;
    - À la fin du programme, des 11 jeunes l'ayant terminé avec succès, tous sont retournés à l'école ou sur le marché du travail;
    - De présenter un total de 114 exposés dans la collectivité et dans les écoles. Ces exposés ont eu un impact important sur les résidents et sur les jeunes, et les organisateurs du programme ont reçu plusieurs témoignages.
- Lors d'une évaluation menée par le NCPC (2009), le programme BTC a été comparé avec d'autres programmes prometteurs sur les gangs aux États-Unis. Il a été démontré que BTC avait des résultats similaires, et dans certains cas, une meilleure étendue que certains autres programmes. Par conséquent, BTC a le potentiel de réaliser des objectifs semblables.
- Le programme a été jusqu'à maintenant offert à 303 jeunes (96 femmes et 207 hommes). Le taux de graduation du programme à temps plein sur 28 semaines est de 74 %.[‡‡]

[‡‡] **Sécurité publique Canada**. 2009, *Le programme Breaking the Cycle Youth Gang Exit and Ambassador Leadership.* Centre national de prévention du crime, Ottawa. Disponible à : http://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/brkng-ccl/index-fra.aspx., en ligne, le 8 février 2021.

Tableau n°1 : MODELE REPRESENTANT LES STRATEGIES POSSIBLES DE DIMINUTION DE LA CRIMINALITE

Stratégie	Cible : population en général (primaire)	Cible : population à risque (secondaire)	Cible : population délinquante (tertiaire)
Prévention (action sur les causes) Développement socio-économique	• Système universel de garderie pour les enfants d'âge préscolaire • Accès à l'éducation	• Programme de soutien auprès de très jeunes mères monoparentales • Soutien aux élèves en difficulté afin de prévenir l'abandon scolaire	• Programme de tutorat communautaire pour ex-détenus • Programme de travaux compensatoires
Réduction des occasions	• Modifications aux normes de construction résidentielle ou aux plans d'urbanisme	• Installation de caméras dans les dépanneurs	• Conditions de libération conditionnelle
Responsabilisation	• Sensibilisation aux toxicomanies • Promotion de l'engagement communautaire	• Campagne contre le vandalisme dans un quartier particulièrement touché • Surveillance communautaire de quartier	• Rééducation de conjoints violents • Médiation • Groupe d'entraide de toxicomanes
Dissuasion	• Barrages routiers contre l'alcool au volant	• Politique à l'égard de la violence conjugale	• Rapidité, certitude et graduation de la peine
Répression		• Resserrement de la surveillance dans certains quartiers	• Opérations spéciales des enquêtes policières

Source : Ministère de la Sécurité publique Québec, https://www.securitepublique.gouv.qc.ca/police/publications

4. AUTOMATISATION DE LA DÉTECTIONNUMÉRIQUE

Sur ce point, avant d'aller plus loin, nous pouvons d'emblée évoquer Le 2ème Forum INTERPOL de criminalistique numérique qui a reconnu que, cette dernière, « appliquée aux équipements de bord des navires, qui a rassemblé 20 représentants des services chargés de l'application de la loi de 10 pays et du secteur privé, avait pour but de présenter les équipements que l'on peut trouver à bord des navires et les méthodes d'extraction de données exploitables dans le cadre d'enquêtes judiciaires »[§§]. Les informations numériques découvertes dans les équipements de bord peuvent être déterminantes pour l'enquête de police.

[§§] https://www.interpol.int/fr/Actualites-et-evenements/Actualites/2019/Using-digital-forensics-to-investigate-maritime-crime, en ligne, le 9 février 2021.

Fig. n°1 : *Equipements de bord des navires maritimes*

Source : www.interpol.int/fr/Actualites-et-evenements/Actualites/2019/Using-digital-forensics-to-investigate-maritime-crime

Malgré que la technologie a un pouvoir habilitant et facilite la criminalité, il est aussi vrai qu'elle peut servir d'outil efficace pour prévenir et détecter la criminalité et les autres urgences, ainsi que d'y répondre. D'autres scientifiques soutiennent même qu'elle favorise de plus une prise de décisions fondée sur des données probantes en matière de sécurité publique.

Ilestégalementpossibled'améliorerlesprocessusetderéduirelesdélaisd'analysedes données numériques en optant pour l'automatisation. Grâce à l'amélioration des technologies de reconnaissance faciale et au progrès constant de la reconnaissance automatique de la voix, des gains d'efficacité importants peuvent être réalisés pour permettre à la Police de résoudre davantage de crimes.

De nos jours, si la Police est munie de la technologie d'analyse de données adéquate, les policiers peuvent analyser eux-mêmes les données d'appareils mobiles, comme les téléphones, les tablettes et les portables, afin de trouver des preuves d'infraction ou de culpabilité sur les auteurs des crimes, plutôt que d'attendre pendant deux ou trois mois que cette analyse soit effectuée par des policiers spécialistes.Si 40 téléphones mobiles sont saisis au cours d'une enquête, il est possible de brancher les téléphones au système d'analyse et de créer une copie de l'ensemble des données desappareils, y compris les noms, numéros de téléphone, adresses électroniques et autres éléments d'information essentielle, à partir des messages texte, des courriels et des applications.

Cesdonnéespeuventêtrerecoupéesaveclesdonnéesgéospatiales,donnantainsiàlapolic eles lieuxd'utilisationdecestéléphones.Grâceàcetteinformation,unenquêteurpeutconclureque six de ces appareils contiennent de l'information pertinente et lui permettront d'établir sa preuve. Il obtient rapidement les données de base nécessaires pour enquêter sur le crime, et le temps des analystes est mieux utilisé puisqu'ils ne devront analyser en détail que les six téléphonesclés.

La technologie permet également l'établissement de liens entre les données, informant les enquêteurs, par exemple, du nombre d'occurrences d'un nom sur certains appareils. Par conséquent, si une personne affirme ne pas connaître l'un des suspects, la preuve est immédiatement fournie par son téléphone. C'est le cas des réquisitions d'expert habituellement utilisées par le Parquet à travers les OPJ.Cette information peut maintenant être récupérée simplement en appuyant sur un boutonplutôt que d'avoir recours à des feuilles de calcul complexes, et améliore l'efficacité de lapolice.

L'analyse des données permet aux corps policiers, selon les leçons tirées de Burgernet Aux Pays-Bas, depuis2010, de :

1. Détecter les points chauds de lacriminalité;
2. Surveiller les médias sociaux à la recherche de risquespotentiels;
3. Suivre l'activité des criminels connus sur les médias sociaux en y cherchant des indices qui pourraient révéler des crimes antérieurs ouplanifiés;
4. Gagner du temps lors de l'analyse des appareils électroniques descriminels.

La police demande l'aide des citoyens pour résoudre les crimes. Pour ce faire, elle leur signalelesincidentsenleurenvoyantunealerteparSMS,partéléphoneouàpartird'unsystème d'information géographique au sein du système Burgernet (« burger » signifiant « citoyen »en néerlandais).Dèsqu'unemployédupostedecommandementestavertid'uncambriolageoude la disparition d'un enfant, il crée une alerte Burgernet. Les participants à Burgernet reçoivent unmessagevocalouun messagetexteleurdonnantunedescriptionclairedelapersonneoudu véhicule afin qu'ils gardent l'œil ouvert. Si un participant aperçoit la personne ou le véhicule en question, il compose le numéro sans frais de Burgernet et est automatiquement mis en communication avec le poste de commandement. L'employé communique ensuite

l'informationauxpoliciers.Lorsquel'incidentestclos,tousceuxquiontparticipéauprocessus Burgernet reçoivent un message leur communiquant les résultats. Grâce aux effortsdesparticipants de Burgernet, des suspects a été pris en flagrant délit, des personnes disparues ont été retrouvées et la police a reçu des renseignements utiles.

Le système a connu un énorme succès ; plus de 1000 appels à l'action sont émis par Burgernet chaque mois, dont 10 % ont conduit à l'arrestation du suspect et 20 % ont conduit indirectement à l'arrestation de criminels.PARTICIPATION CITOYENNE ACCRUE. L'accroissement de la participation citoyennecontribueàétablirlaconfianceauseindelacollectivitéetàlaconserver.Lescitoyens deviennent des partenaires connus qui servent de « capteurs sociaux » pour la police. ComProNet, (« Community Protection Network »), un autre projet néerlandais visant à réduire la criminalité liée aux incidents locaux, est également à l'essai en Belgique.L'object

II. L'UTILISATION DES LOGICIELS

Avec l'avènement de l'informatique, il existe des enjeux soulevés par l'usage des algorithmes prédictifs en matière de sécurité publique. Ces enjeux sont à la base de la *Police Prédictive*. La volonté de la prédiction dans les services de Police a pris beaucoup d'ampleur avec cette ère de Bid data dans la mesure où cette notion promet des réponses plus exhaustives et efficaces. Plusieurs recherches en France ont montré qu'avec l'enregistrement systématique des données ainsi que la multiplication de la traçabilité digitale dans la société génère une transformation des rationalités qui constituent des stratégies et des tactiques de gouvernements (Rouvroy A., Berns T., 2010).

En France et aux Etats-Unis, la Police prédictive est devenue plus prononcée par les recherches des scientifiques sociologues ou autres et même dans la pratique des interventions policières. A ce sujet, l'Institut d'Aménagement et d'Urbanisme de la région d'ÎLE-DE-France nous fait savoir qu'« Au même moment, aux États-Unis, la police prédictive se développe et de nombreuses polices américaines ont recours à des nouveaux logiciels en ce sens. Le plus connu est développé par une *start-up*, Predpol, qui commercialise un logiciel d'anticipation des faits de délinquance. Son objectif : permettre d'orienter les patrouilles sur des zones identifiées « sensibles » et éviter le passage à l'acte du criminel. Présentée sous forme de cartes de chaleur représentant la répartition spatiale

de la délinquance, l'innovation de Predpol repose sur l'usage d'un algorithme qui, pour rendre la police plus proactive, … »[***].

Nous notons de ce meme auteur que « l'algorithme fonctionne comme un outil de gestion de l'action des policiers. Il oblige les patrouilles de police à passer 5% de leur temps disponible dans les zones à risques identifiées (des carrés rouges de 200 mètres sur 200 mètres). Ce dosage du temps de présence des policiers est effectué en temps réel et selon les secteurs de la ville. Cette rationalisation des interventions des agents de police va de pair avec une réflexion plus globale de retour sur investissement. Pour que l'algorithme puisse prioriser les interventions et orienter les patrouilles, il s'agit de calculer de façon pragmatique le coût de l'intervention de la police (agents mobilisés, durée de l'enquête, etc.), et *in fine* le coût de la criminalité pour la société civile ».[†††]

Fig. 2 : Le service de data-scientist de la gendarmerie nationale

Source : *Camille Gosselin / La police prédictive, 2019*

Dans les paragraphes qui suivent, nous présentons, à titre illustratif, quelques techniques ou logiciels au service de la Police.

Quelques techniques de la Police prédictive :

- Algorithme

Description d'une suite finie et non ambigüe d'étapes ou d'instructions permettant d'obtenir un résultatà partir d'éléments fournis en entrée.

- Apprentissage automatique ou *Machine learning*

[***]Gosselin, C.,*La police prédictive. Enjeux soulevés par l'usage des algorithmes prédictifs en matière de sécurité publique / IAU îdF*, Paris, Ed. Cedex, 2019, p. 4.
[†††]Gosselin, C., Op. Cit., p.4

Branche de l'intelligence artificielle, fondée sur des méthodes d'apprentissage et d'acquisitionautomatique de nouvelles connaissances par les ordinateurs, qui permet de les faire agir sans qu'ilsaient à être explicitement programmés.

- *Big data*

Désigne la conjonction entre d'une part, d'immenses volumes de données devenus difficilementtraitables à l'heure du numérique et, d'autre part, les nouvelles techniques permettant de traiter cesdonnées, voire d'en tirer par le repérage de corrélations des informations inattendues.

- Biométrie

Regroupe l'ensemble des techniques informatiques permettant de reconnaître automatiquement unindividu à partir de ses caractéristiques physiques, biologiques, voire comportementales. Les donnéesbiométriques sont des données à caractère personnel car elles permettent d'identifier une personne.

Elles ont, pour la plupart, la particularité d'être uniques et permanentes (ADN, empreintes digitales,etc.).

- Intelligence artificielle

Théories et techniques « consistant à faire faire à des machines ce que l'homme ferait moyennant unecertaine intelligence » (Marvin Minsky). On distingue IA faible (IA capable de simuler l'intelligencehumaine pour une tâche bien déterminée) et IA forte (IA générique et autonome qui pourrait appliquerses capacités à n'importe quel problème, répliquant en cela une caractéristique forte de l'intelligencehumaine, soit une forme de « conscience » de la machine).

- Reconnaissance faciale

Une technique qui permet à partir des traits de visage :

- d'authentifier une personne : c'est-à-dire, vérifier qu'une personne est bien celle qu'elle prétend être(dans le cadre d'un contrôle d'accès), ou
- d'identifier une personne : c'est-à-dire, de retrouver une personne au sein d'un groupe d'individus,dans un lieu, une image ou une base de données.

III. LA TELESURVEILLANCE

« Les équipements électroniques de détection et d'alarme installés dans les établissements n'ont d'intérêtque si l'alerte est suivie d'une intervention »[‡‡‡],

‡‡‡ ANGOT, S. et Consort, *Conception d'un système de vidéosurveillance pour l'IMT*, Projet Transverse, Marseille, S.E., S.D., p.1

déclarentSébastien Angot et consort. Cette déclaration démontre à suffisance le rôle de la Police dans le Système de télésurveillance. La télésurveillance est définie par le *Centre Scientifique et Technique du Bâtiment (ROCHETTE, MARCHANDET, 1998, p. 7) comme : « « la surveillance à distance d'un local ou d'installations techniques (chaufferies, vitrines réfrigérées, chambres froides, éclairages) ; elle est le plus souvent effectuée par un prestataire de service distant, le télésurveilleur*[§§§] *»*

Dans la sécurité, spécialement à la Police, la télésurveillance est plus exploitée dans son approche vidéosurveillance qui reste sa forme la plus connue. La mise en place d'une installation de vidéosurveillance passe par une analyse très précise afin de répondre aux exigences et aux besoins de l'utilisateur qu'est la population d'une ville ou des bâtiments.

Elle permet ainsi de : surveiller,

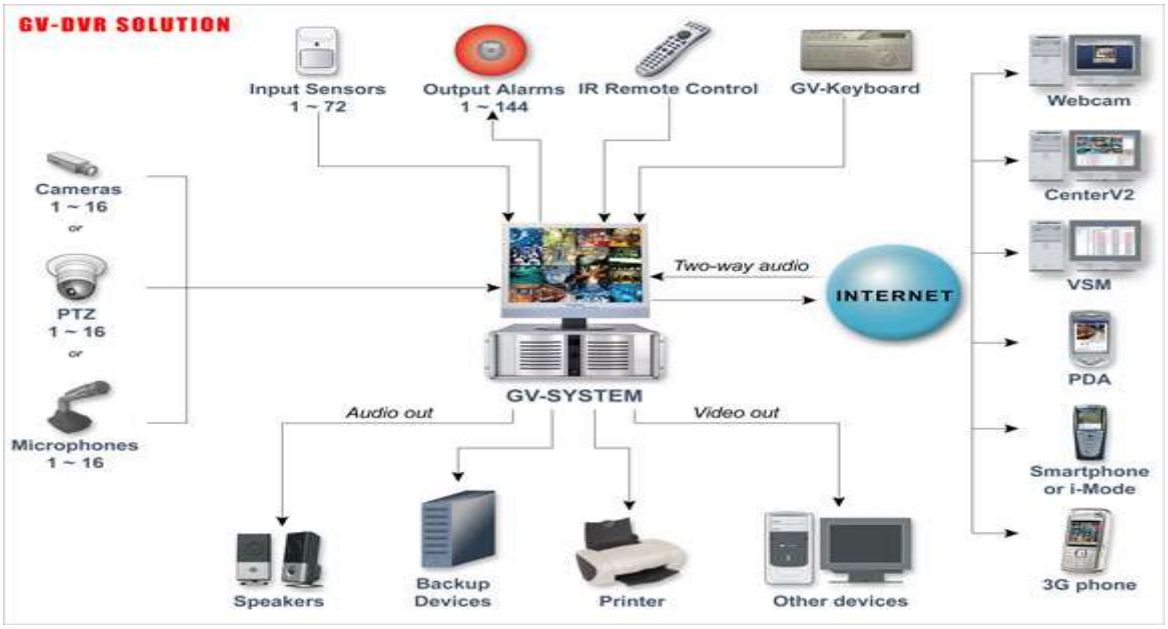
- reconnaître,
- identifier,
- contrôler,
- protéger,
- alerter,
- détecter,
- sécuriser,
- superviser,
- enregistrer,
- archiver,
- consulter,
- transmettre,
- analyser, etc.

Trois grandes technologies sont d'usage pour l'application de la vidéosurveillance, notamment : IP, HD-SDI et analogique. Nombreux sont les types des systèmes de vidéosurveillance dont ; Système sur réseaux IP, système analogique, GV-Series de GeoVision et Système< hybride > de vidéosurveillance.

Dans cet article et en rapport avec la Police, deux systèmes sont recommandables selon en fonction de leur efficacité et selon les moyens et les compétences techniques dont dispose le Ministère de l'intérieur et de sécurité. Nous retenons, pour ce, le système hybride qui intègre les systèmes classiques de vidéosurveillance basés sur les caméras analogiques et les caméras en réseau et le système Geovision qui est un système multicanal de surveillance vidéo sous PC qui utilise les technologies de compression vidéo numérique les plus avancées afin de vous apporter la meilleure qualité d'image et les meilleures performances vidéo mieux indiquées pour les preuves.

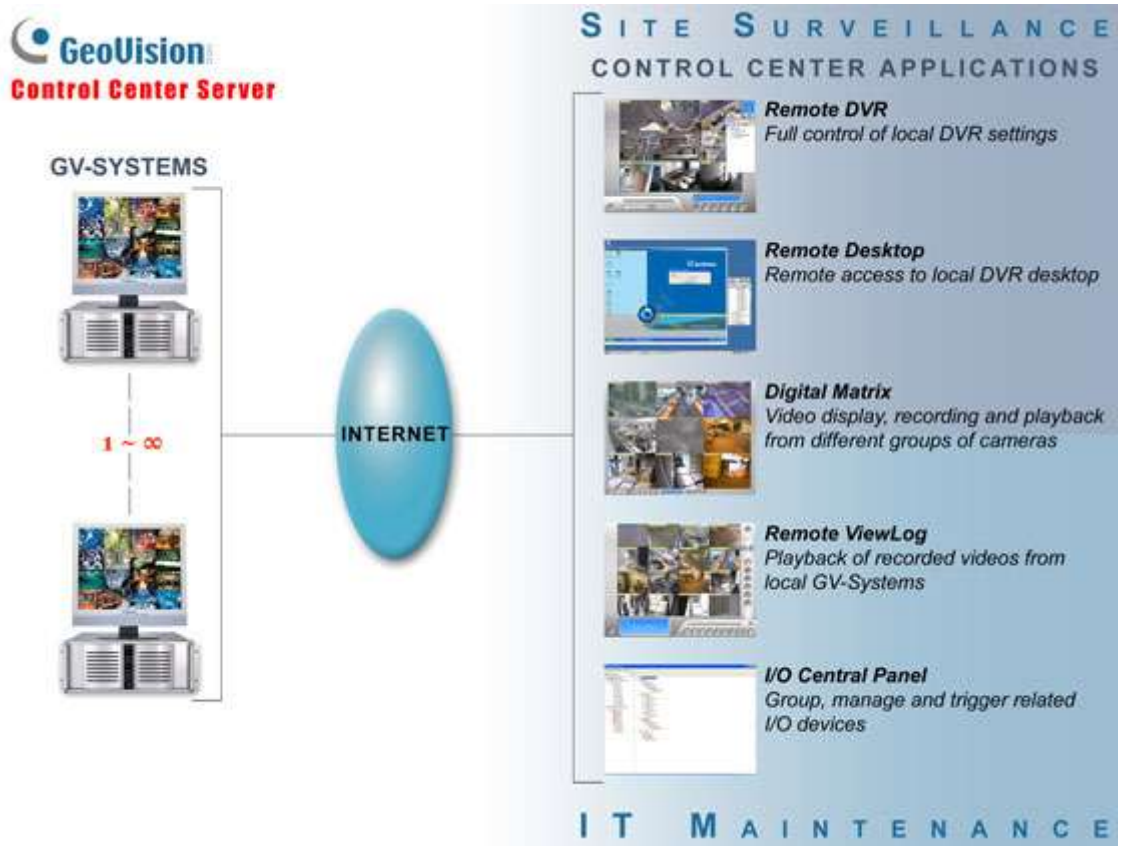
[§§§] *Démocratie et télésurveillance - Introduction. Acceptabilité de la télésurveillance* - Presses universitaires du Septentrion (openedition.org), https://books.openedition.org/septentrion/51628?lang=fr, en ligne, le 10 Février 2021.

Fig. 3 : Modèle d'architecture d'un système hybride



Source : www.techno-science.net

Fig. 4 : **GV-Series de GeoVision**



Source : www.techno-science.net

5. CONCLUSION

Le modèle traditionnel des services de Police n'est plus approprié à notre société en constante évolution. La criminalité se métamorphose avec les changements des mentalités des criminels ainsi que l'environnement technique et social. L'adoption d'une nouvelle approche serait la suite logique de l'amélioration continue des services de Police pour répondre aux perpétuels besoins de la société. La croissance rapide delamêmetechnologiequiestàl'originedesnouveauxdéfisenmatièred'applicationdelaloi crée également de nouvelles occasions d'optimiser les interventions et l'efficacité des services deSécurité.

Lesactivitésdetransitionverslanouvellegénérationdeservicesdepolicepeuventtirer parti des meilleures pratiques existantes et des techniques novatrices en déploiement abordées dans le présent article, notamment:

1. Les services de police fondés sur lesrenseignements;
2. Les modèles d'échange de données pour soutenir la collaboration entre lesorganismes publics et privés;
3. Les nouveaux canaux de communication augmentant la participationcitoyenne;
4. Les solutions mobiles favorisant l'efficacité du déploiement desressources;
5. L'analytique prévisionnelle contribuant à la lutte contre lacybercriminalité.

Latechnologiepeutêtretrèsefficacepourdéployerlesressourcesdefaçonadéquate,entemps réel, opportunetàl'endroitapproprié.Elleconstitueuneapprochecibléesurlescrimestraditionnels etvirtuels.

Nous observons un changement de cap dans la façon dont les organismes, les citoyens et la Police collaborent. La technologie appropriée continuera de favoriser l'échange d'information entre toutes les parties.

Lorsque les policiers sont avisés de la présence d'enfants à l'étage d'une maison où ils se présentent pour un cas de violence conjugale, ou qu'un groupe d'amateurs sportifs chahuteurs cherchent les ennuis, ils sont mieux renseignés et ont la possibilité d'adopter une approche proactive. Ainsi, la Police peut intervenir avant qu'un crime soit commis et économiser du temps et de l'argent, empêcher la souffrance des citoyens et même sauver des vies sans trop des tâtonnements.

Unregardneufsurlesméthodesdetravailrévèleradenouvellesoccasionsd'innoveren vue d'accroître la collaboration de la Police avec d'autres organismes et les citoyens afin de créer une société réellement plus sécuritaire pour l'ensemble de lapopulation.

BIBLIOGRAPHIE SELECTIVE

I. OUVRAGES

1. ANGOT, S. et Consort, *Conception d'un système de vidéosurveillance pour l'IMT*, Projet Transverse, Marseille, S.E., S.D.
2. BRODEUR, J.P., Les visages de la Police. Pratiques et Perceptions, Montréal, Ed. P.U.M., 2003.
3. Chemla, A., « Réprimer les infractions numériques : une tâche lourde et lente », in *Sécurité globale2019/3 N° 19*
4. **Frantz** Denat, « Prévention… Le rôle de la police », in *revue internationale d'éthique sociétale et gouvernementale*, vol. 4, n° 2 | 2002.
5. Gosselin, C., *La police prédictive. Enjeux soulevés par l'usage des algorithmes prédictifs en matière de sécurité publique / IAU îdF*, Paris, Ed. Cedex, 2019.
6. **Sécurité publique Canada,***Le programme Breaking the Cycle Youth Gang Exit and Ambassador Leadership*. Centre national de prévention du crime, Ottawa, 2009.
7. UNIDIR, *The Cyber Index : International Security Trends and Realities*, United Nation Institute for Disarmament,Research, Genève & New York, 2013.

II. AUTRES DOCUMENTS

1. NATIONS UNIES POLICE Office contre la drogue et le crime,*Sécurité publique et prestation des Services de police ; Compilation d'outils d'évaluation de la justice pénale*, New York, 2008.
2. Police Nationale Congolaise (PNC), LOI ORGANIQUE PORTANT ORGANISATION ET FONCTIONNEMENT DE LA POLICE NATIONALE CONGOLAISE, Journal Officiel, Kinshasa, 11 Août 2011.
3. DGRIS-MINISTERE DE LA DEFENSE, *Description de la manière dont la cybercriminalité et la lutte informatique sont abordées par les acteurs pouvant influencer le domaine*, Compagnie Européenne d'Intelligence Stratégique (CEIS), Mars 2015.

I. WEBOGRAPHIE

- www.cairn.info/revue-securite-globale-2019-3-page-39.html
- www.andre-clarinval.be › pages › journal
- www.techno-science.net
- https://journals.openedition.org/ethiquepublique/2201
- http://www.cantraining.org/BTC/docs/Sawdon%20Evans%20CT%20Artic

le.pdf
- http://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/brkng-ccl/index-fra.aspx
- https://www.interpol.int/fr/Actualites-et-evenements/Actualites/2019/Using-digital-forensics-to-investigate-maritime-crime
- https://www.securitepublique.gouv.qc.ca/police/publications
- https://books.openedition.org/septentrion/51628?lang=fr