Infoprisons
Plateforme d'échanges
sur la prison et la sanction pénale

Mars 2021

Rapport du Congrès de Criminologie SAK/GSC 2020 à Interlaken

Le Congrès de Criminologie Suisse 2020 a eu lieu entre le 30 septembre et le 1er octobre et a abordé le thème « La justice pénale entre intelligence artificielle et algorithmes prédictifs dans le but ultime de la numérisation totale de la justice ». Cet article vous propose un compte-rendu des questions abordées lors du Congrès.

Le congrès démarre avec l'exposé du Prof. Philippe Cudre-Mauroux (UNI Fribourg) qui déclare :

Pour la numérisation de la justice, nous avons besoin de l'Intelligence Artificielle (IA)

«Mais», concède Ph. Cudre-Mauroux, «l'efficacité de l'IA ne rencontre aucun consensus auprès des expert(e)s. Les un(e)s sont confiant(e)s, les autres pas du tout. Alors : entre confiance aveugle et peur panique, que penser ? Même si les ordinateurs apprennent de mieux en mieux à gérer des algorithmes, les erreurs déjà prévisibles aujourd'hui ne seront peut-être pas corrigées demain dans le processus recherché d'accélération des prises de décision. Il faut juste admettre que pour tenter de diminuer les erreurs dans les processus de numérisation, la gestion de milliards de paramètres et de données sera nécessaire, utilisant des capacités de stockage énormes. Énormes masses de données qui, en cas de bug, augmenteront les risques d'erreur. Sans que l'utilisateur du logiciel ne s'en rende nécessairement compte. Et la sécurité de stockage des données ? »

L'orateur cite le Prof. P. Domingos: « Les gens ont peur que les ordinateurs deviennent trop malins, mais le vrai problème est que les ordinateurs sont stupides et dominent déjà le monde… ».

Le Prof. Dr. Philippe Gilliéron, avocat, prof. aux Universités de Lausanne et Fribourg continue avec la question

Justice pénale et Intelligence Artificielle : qu'en penser ?

Philippe Gilliéron cite quelques exemples d'application de l'IA en parlant d'emblée de la reconnaissance faciale (RF) dans les rues de grandes villes en Chine. Au Xinjiang, la RF est utilisée largement pour la répression des Ouïgours par le système chinois Hikvision. Dans d'autres pays comme aux Etats Unis, certaines caméras de surveillance privées sont déjà connectées à des centrales d'analyse avec reconnaissance faciale. La maison de vente par correspondance Amazon utilise depuis longtemps la reconnaissance faciale et vocale pour « sécuriser » les achats par téléphone portable. D'ailleurs, Amazon vend son service RING avec ses techniques de reconnaissance à la Police américaine et a réalisé en 2019 un chiffre d'affaires de 2 milliards de dollars dans ce domaine.
« Toujours aux USA et dans la recherche de prévisibilité de la criminalité par la police (p. ex. : patrouiller dans quel quartier ?), les grandes villes utilisent des cartes géographiques numériques prédictives et modifiées en temps réel, cartes «intelligentes» nourries par des statistiques et des alarmes déclenchées. Mais les caméras de surveillance connectées aux serveurs de reconnaissance faciale sont à l'origine d'erreurs fréquentes. La reconnaissance faciale du visage d'un Afro-Américain fonctionne moins bien qu'avec un visage blanc. D'autre part, l'analyse faciale numérique ne serait pas encore capable de prendre en compte l'aspect émotionnel du visage (joie ou angoisse?) ni le langage corporel. Il en résulte une concentration erronée d'interventions dans certains quartiers et d'arrestation de personnes qui avaient juste le tort d'être là au mauvais moment. Même si ces personnes, injustement suspectées, sont finalement libérées, elles occupent inutilement les tribunaux, nourrissant les statistiques prédictives de chiffres faussés par des biais répliqués ».

Dans l'affaire de l'état de Wisconsin contre Loomis, 881 N.W.2d 749 (Wis. 2016), la question suivante avait surgit: « Un individu peut-il contester le résultat donné par un algorithme, motif étant tiré du fait qu'il contreviendrait à un procès équitable ? » Finalement, la cour avait admis dans cette affaire les résultats fournis par la reconnaissance faciale.

San Francisco est la seule ville aux USA qui a renoncé à la reconnaissance faciale (état fin 2020).
En attendant, l'Allemagne envisage le déploiement de caméras à reconnaissance faciale dans 134 gares et 14 aéroports et la France projette des systèmes analogues.
Conclusion du Prof. Philippe Gilliéron : « Nous pourrons aller vers une justice avec le danger

- d'un passage de la causalité à la simple corrélation comme moyen de preuve,
- d'une non-observation de la présomption d'innocence,
- d'une individualisation des peines (art. 27 CP),
- de passer à une justice punitive

négligeant l'aspect de réhabilitation,
- d'un rôle croissant joué par des acteurs privés dans des domaines réservés à des acteurs publics.

Donc, tous les acteurs doivent reconnaître le besoin de réglementer le recours aux systèmes d'Intelligence Artificielle ».

Le Dr. Prof. Patrik Manzoni, de la Zürcher Hochschule für Angewandte Wissenschaften, Institut für Delinquenz und Kriminalprävention, nous parle des **résultats d'une recherche sur les Bodycams testés par la Police urbaine zurichoise en 2017.**

Cette enquête repose sur un questionnaire libellé par des policiers/ères urbain(e)s et sur des interviews après l'utilisation de ces appareils pendant 3 mois. Les conditions d'utilisations avaient été précises :

- pas d'utilisation dans la sphère privée,
- caméra bien visible et obligation d'avertissement avant enclenchement,
- enregistrement seulement en cas d'escalade lors d'une intervention,
- l'appareil enregistre automatiquement 30 secondes avant enclenchement grâce à une mémoire « circulaire » (dans la réalité, la mémoire enregistre tout le temps en effaçant continuellement ce qui est antérieur à 30 secondes).

Après le retour des 88,3% des questionnaires et la fin des interviews, une analyse sommaire donne les résultats suivants :

- bonne acceptation des Bodycams par les policiers/ères,
- la plupart des policiers/ères parlent d'une bonne possibilité de présentation de preuves,
- quelques-uns/unes évoquent la fonction de désescalade lors d'interventions,
- constat d'une baisse d'agressions envers les policiers/ères.

Concernant les agressions, une analyse (purement statistique) avec calcul sur une année de 52 semaines et 23'507 interventions donne les chiffres suivants :

- sans Bodycams = 136 agressions (0,58%),
- avec Bodycams = 89 agressions (0,38%), donc 47 agressions pourraient théoriquement être évitées, soit environ un 1/3.

Ci-après les impressions négatives exprimées par les policiers/ères :

- éventuelle retenue dans les situations demandant une action plus énergique - les policiers/ères se sentent contrôlé(e)s,
- un certain stress à cause de « l'obligation d'un langage plus élaboré »,
- peur d'un plus grand risque de critiques/sanctions par les supérieurs,
- constat d'un effet « calmant » plus limité auprès de personnes ivres ou droguées.

Déjà à ce stade (2018), la police urbaine de Zürich a décidé, dans un futur proche, d'équiper les policiers/ères avec les Bodycams.

L'orateur termine avec la remarque qu'au vu de ce qui précède, une réglementation précise concernant l'accès aux enregistrements devrait être élaborée avant l'adoption généralisée des Bodycams.

M. Yves Nicolet, Procureur, Ministère public de la Confédération évoque les **Défis légaux et pratiques posés par la lutte contre la cybercriminalité.**

« Depuis quelques années, nous observons une baisse de la criminalité en Suisse – excepté dans la cybercriminalité. Pour contrer cette dernière, des outils et procédures sont à renforcer ou à mettre en place ».
Yves Nicolet décrit les difficultés en matière de cybercriminalité à l'exemple du Pharming, une sous-catégorie du Pishing (= installation d'un logiciel « malveillant » dans l'ordinateur de la victime, p. ex. par une pièce jointe afin de prendre le pouvoir sur l'ordinateur).
« Le Pharming dirige la victime, après la prise de pouvoir sur son ordinateur, vers une fausse page d'internet (p. ex. sa banque) pour détourner de l'argent. Une société-écran recrute des Money-mules qui récupèrent les montants et les redistribuent. Les Money-mules sont rétribuées. La traque du Pharming est techniquement très difficile. Ci-après les difficultés des plans techniques et juridiques pour contrer cette criminalité :

Plans techniques :

- Compréhension des phénomènes (Phishing, Pharming, DDoS, Darknet, etc.),
- traces numériques éphémères (délai de conservation IP),
- procédés d'anonymisation (Spoofing, VPN, Proxy, TOR, mails jetables),
- cryptage des communications (WhatsApp, Skype, etc.),
- téléphonie par Internet (VoIP).

Plans juridiques :

En l'absence de définitions légales encore à l'heure actuelle, la cybercriminalité est définie au sens large par la liste FEDPOL. La police est aidée dans cette tâche par la Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI à Berne[1].
Par la pluralité des lieux de commission des délits du Pharming (les auteurs

principaux sont à l'étranger, le vol de l'argent des victimes concerne plusieurs cantons en Suisse), la compétence en la matière sont le MPC (Ministère public de la Confédération) et le MP (Ministère public) des cantons[2].
En ce qui concerne la qualification juridique de la cybercriminalité, il existe déjà un certain nombre de lois (art. 143, 143bis, 144bis, 197 al. 5 CP not.). Contre le Pharming : art. 143, 143bis, 144bis, 147 et 305bis CP, et contre les Money mules en Suisse art. 3 du CP ».
D'autres lois spéciales restent encore à créer.

Les perspectives d'avenir sont la concrétisation de CYBERBOARD, qui sera

- stratégique : l'organe de pilotage Cyber STRAT sera utilisé par les différents intervenants comme p. ex. MPC et Fedpol,
- opératif : l'élément principal Cyber-CORE sera utilisé pour la coordination, coopération, consultation et communication entre les différents intervenants comme p. ex. entre le MPC et Fedpol avec l'outil MELANI.

Les affaires seront initiées et contrôlées par les volets Cyber-CASE (vu l'ensemble des affaires) et Cyber-STAT (état de la situation).
Dans sa séance du 25 février 2019, la Conférence des commandants des polices cantonales de Romandie, Berne et Tessin (CCPC RBT) a décidé la création d'un Centre de Compétence Cyber (CCC) **PICSEL** : **P**lateforme d'**I**nformation de la **C**riminalité **S**érielle **E**n **L**igne.
A noter que sur le plan européen, The European Judicial Cybercrime Network **EJCN** a été créé le 9 juin 2016.
Le Dr. Jens Piesbergen, chef du programme HIS (Harmonisation de l'informatique dans la justice pénale) et chef-adjoint de projet Justitia 4.0, KKJPD, Berne, explique le planning pour concrétiser Justitia 4.0 sous le titre :

Conception et implications de la numérisation de la justice

En introduction, un extrait du texte que l'orateur a écrit dans l'annonce de son exposé :
« Le projet *Justitia 4.0* a été lancé par la Conférence Cantonale de Justice et de Police (CCDJP) et les tribunaux afin de simplifier la communication électronique et de généraliser le dossier électronique auprès des autorités de poursuite pénale et des tribunaux sur l'ensemble du territoire, afin de faciliter l'accès à la justice avec des effets positifs sur l'efficacité et la qualité, et on améliore également l'attractivité de la justice en tant d'employeur.
Dans le projet *Justitia 4.0*, ce ne sont pas les aspects techniques ou juridiques qui posent les plus grands défis, mais bien l'aspect humain. Nous sommes toutefois certains que, d'ici à quelques années, la Suisse sera en mesure d'offrir à ses habitants un système judiciaire efficace et facilement accessible par voie électronique ».

« Transformation digitale : quels changements voulons-nous atteindre ? Voici un aperçu :

- Place de travail entièrement digitale et donc indépendante d'un lieu fixe,
- documents numérisés (e-documents),
- interopérabilité entre documents, métadonnées et archivage,
- signature(s) numériques des autorités et acteurs judiciaires (E-ID),
- modèles d'utilisation des données, séparation entre données et applications,
- centralisation et redistribution des données sur site,
- programmes avec assistance SaaS (Software as a Service),
- gouvernance des données par les acteurs judiciaires concernés,
- contrôle automatique des délais,
- développement et recherches d'améliorations en commun.

Les acteurs judiciaires ne travailleront plus qu'en réseau ! »
« Le programme HIS sera concrétisé par un échange de données sécurisées avec des processus sans coupures entre les différents acteurs judiciaires, cantons, confédération et tiers professionnels.
Le plan d'action pour *Justitia 4.0* se base sur les travaux initiés en 2018. Voici la chronologie des acquis et des prévisions (état sept. 2020) :

- 2019-2020 : présentation des concepts, tests « en bacs à sable », contrôle des cahiers des charges par groupes de travail, consultations entre groupes d'experts (techniques et juridiques), demande de soumissions aux entreprises de programmes, plans de financement et élaboration des budgets.
- 2021-2022 : recueil des expériences en « bacs à sable », minimisation des risques, confrontation concept vs cahier des charges, rédaction catalogue des critiques, échanges entre experts, 1ers tests pilote, processus parlementaire.
- 2022-2024 : période de transition, d'écolage et de support aux acteurs ; les premiers cantons se lancent en cycles adaptés au terrain, répétition de la confrontation concept vs cahier des charges, rédaction catalogue des critiques, échanges entre experts, surveillance en continu des budgets.
- 2025-2026 : *Justitia 4.0* devient obligatoire.

Tous les dossiers seront gérés par e-ID (identité électronique) y compris l'agenda, les demandes des avocats, les expertises demandées, etc.

jusqu'à l'entrée des données dans les statistiques ».
Dans la discussion ouverte qui suivait cet exposé, la question posée la plus pertinente était : « Comment se mettre d'accord sur les **définitions**, sachant que 5 juristes proposent 5 définitions différentes ? ».

Exposé de M. René Bühler, notaire, directeur adjoint FEDPOL

Lutte contre le terrorisme dans un monde de technologies contemporaines

René Bühler rappelle qu'à la veille du congrès, le 25.09.2020, le parlement a voté une nouvelle loi cadre pour faciliter la lutte contre le terrorisme.
Il nous cite le cas du jeune Chérif C. soupçonné d'une attaque sanglante à Strasbourg. Chérif C. avait commis auparavant plusieurs cambriolages en Suisse, et cela dans cinq cantons.
« Le défi à prévenir de telles attaques réside dans la difficulté de suivre ces personnes transfrontalières. Les communications avec leur réseau ou complices se font en numérique et cryptées (p. ex. Whatsapp).
Pour la police, les défis opérationnels sont tout d'abord la découverte puis le suivi de ces communications. Ce n'est souvent qu'après la détection d'une personne suspecte ou même arrêtée que la police peut analyser les portables séquestrés et demander l'entraide aux opérateurs téléphoniques. La collaboration entre cantons est primordiale. Ces recherches sont longues et fastidieuses.
Statistiquement, le terroriste moyen est de sexe masculin, âgé d'environ 30 ans et présente, pour un tiers, un passé de délinquant. Le recrutement et l'endoctrinement se fait beaucoup par Internet. 30% d'entre eux ont passé à l'acte après un événement personnel négatif.
Pour tout cela, certains nouveaux défis juridiques sont demandés à nos autorités, comme par exemple la possibilité de poursuivre quelqu'un qui s'est rendu dans un « pays de recrutement ». De meilleurs échanges entre entités (polices, cantons, confédération) deviendront obligatoires. Toute la société est responsabilisée – et suspecte ! »

M. Jörg Arnold, physicien ETHZ, directeur adjoint de l'Institut forensique de Zürich disserte sur

Les algorithmes : entre confiance aveugle et peur panique

Jörg Arnold rappelle que l'intelligence artificielle peut nous aider, mais
doit-elle toujours nous soutenir pour une décision ?
qui programme, qui contrôle les algorithmes prédictifs « iudex non calculat ? »
devrons-nous tourner notre regard vers le futur ou vers le passé (le problème du « temps » comme 4ème dimension) ?

« D'après l'art. 139 CPP (Code de procédure pénale), principe 1 (interprétation) :
Dans la recherche de la vérité, les autorités judiciaires utilisent toutes les preuves utilisables qui sont, dans l'état actuel des sciences, juridiquement admises.
Mais où sont les limites de la recevabilité ? »
« Le problème de l'inversion du temps dans l'enquête criminelle est que le résultat est déjà la réalité. Les recherches regardent en arrière (qu'est-ce qui s'est passé ?).
Mais il serait beaucoup plus intéressant de savoir quelle était la situation à l'origine de l'événement ou du délit ?
Dans le 4ème théorème sur la théorie des probabilité, Thomas Bayes oppose les hypothèses de l'accusation et de la défense[3] :
situations conditionnelles, documents, témoignages, probabilités au départ (à priori), résultat des recherches forensiques et leur niveau de valeur de preuves, adaptation aux convictions personnelles et la probabilité finale (à postériori).
Mais, finalement, le forensique est factuel, le juriste argumente ! Et où se cache le facteur temps ?
Avec les probabilités conditionnelles, on s'intéresse aux faits qui dépendent d'un événement antérieur. Le point de vue forensique dépend d'une trace qui pourrait être causée par l'accusé(e). Ce point de vue est perçu et argumenté par l'accusation comme preuve.
Dans le cas de la reconstitution d'un accident, l'algorithme de l'évitabilité essaie de calculer avec les données spatiales, de vitesse, d'état de la route, de visibilité, etc. si le conducteur a roulé à une vitesse adaptée ou non, s'il a tardé à réagir/freiner à la vue de la situation dangereuse, si la situation, en variant les différentes données, aurait été maîtrisable. (La variation d'une seule donnée est admise).

Nous avons donc des exigences précises envers les algorithmes. Pour pouvoir y faire confiance, il nous faut de la transparence avec de la documentation complète, la traçabilité face aux bases scientifiques, la vérifiabilité avec des données de test et la définition des conditions cadre de leur utilisation ».

Jörg Arnold nous invite à ne pas faire preuve d'une confiance aveugle à l'IA, mais de rester intéressé et critique. « Restons humbles », dit-il. « Prétendre à une exactitude est impossible ».

Dr. Raquel Rosés, post-doctorante au Mobiliar Lab for Analytics, ETH Zürich, nous entretient sur

Prédire la criminalité - méthodes et données

« Dans le souhait de vouloir prédire

la criminalité, des algorithmes de prédiction spatio-temporels sont utilisés. Avec l'aide de données statistiques de criminalité et données géographiques de la police, nous cherchons à trouver des endroits d'accumulation d'événements (hot spots), où il y aurait donc un plus grand potentiel de risques. Des logiciels comme p. ex. PredPol, HunchLab sont déjà en service auprès des polices aux États Unis, ou comme par exemple Precobs en Allemagne.
Ces logiciels ne sont pas sans défauts, bien-entendu. Des données récoltées par la police peuvent être biaisées, car collectées avec les différentes interprétations personnelles selon les agents qui les ont éditées. Un autre risque se trouve dans la création artificielle de ces « points chauds » par des interventions persistantes dans certains quartiers, interventions plus ou moins fructueuses qui vont auto-alimenter les statistiques. La suspicion permanente risque d'y créer une situation de tension qui peut susciter des violences entre citoyens et forces de l'ordre (délits de faciès).
Qui va ensuite porter la responsabilité des biais ainsi créés ? La police qui suit aveuglément les indications prédictives ou les fournisseurs des logiciels ? Des fournisseurs pourraient êtres tentés par une programmation « efficace » montrant des dangers surévalués. Il est également difficile de comparer l'efficacité des programmes prédictifs avant l'achat ».
La conférencière détaille ensuite les différents canaux de récolte d'informations :

- démographiques, comme par exemple densité et âge de la population d'un quartier donné,
- genre de lieu donnant l'occasion à des fréquentations accrues (événements, fêtes),
- nombre de participants et contexte de ces activités (sans données individuelles).

Dans son travail de recherche pour créer un modèle prédictif pour a) le canton d'Argovie et b) la ville de New York, USA, Raquel Rosés révèle ci-après ses sources de données :

- pour l'action humaine (spatio-temporelle) : a) events.ch, b) Foursquare[4]/N.Y.Subways,
- pour les endroits géographiques intéressants : a) Open Street Map, b) Foursquare,
- pour les facteurs sociodémographiques : a) Confédération Suisse, b) CENSUS[5],
- pour les crimes et délits : a) police cantonale d'Argovie, b) N.Y. City Open Data.

Finalement, deux mêmes cartes géographiques de New York City datant de 2018 sont présentées. L'une montre, par des tâches en rose et rouge en intensités variables, le résultat du modèle de prédictions criminelles dans certains quartiers. L'autre montre les résultats de la criminalité réelle par les mêmes couleurs en dégradés.
La similitude entre prédictions et réalité est étonnante.

Pour terminer ce congrès, un exposé diffusé par visioconférence
du Prof. Dr. Phil. Jean Lassègue, philosophe des sciences, chercheur au CRNS (France)

Justice digitale, les effets des algorithmes sur la justice

L'orateur se livre à une analyse épistémologique sur la transformation de la justice par la numérisation. Son exposé peut être résumé en quelques phrases :

- La justice digitale est le théâtre d'un affrontement entre deux manières de produire du sens et d'organiser la coexistence humaine.
- Le droit digital représente un refus des rapports sociaux et est soumis, dans une société post-libérale, à une stratégie du coût - bénéfice.
- Même les juristes expérimentés se trouvent comme des analphabètes devant le codage des textes légaux – il y a là un nivellement par le bas qui pose problème.
- Entre les informaticiens et les juristes il y a un abîme, et c'est cela qui a un effet sur la légalité et peut produire un texte juridique qui échappe au législateur et à l'utilisateur.
- A partir d'un certain moment, la loi n'est plus un texte, mais un code – non pas un code civil mais bien un code informatique. La loi devient donc illisible pour le citoyen ; elle n'est plus intégralement rédigée par les professionnels du droit.

A méditer...

■ Michel Finazzi

Notes

1. https://www.melani.admin.ch/melani/fr/home/themen.html
2. Art. 24 al. 1 CPP -TPF : BG.2011.27, notamment MPC art. 8 CP (Code pénal)
3. Le 4ème théorème de Thomas Bayes sur la théorie des probabilités décrit le calcul des probabilités conditionnelles.
4. Plateforme américaine de recherche de lieux commerciaux et sociaux
5. Bureau de recensement des habitants aux USA