

**Article - L'IA AU SERVICE DE LA SÉCURITÉ**

PSM - N° 249 - Septembre/Octobre 2018



**dossier**

# L'IA au service de la sécurité

L'IA et ses possibles applications dans le monde de la sécurité sont plus que jamais d'actualité. Et le seront de plus en plus. Alors, certes, on en parle beaucoup, mais que recouvre concrètement l'IA et que permet-elle? Que permettra-t-elle demain? Et dans quelles limites?



© Getty image

**SOMMAIRE** → L'IA: utile mais sous certaines conditions

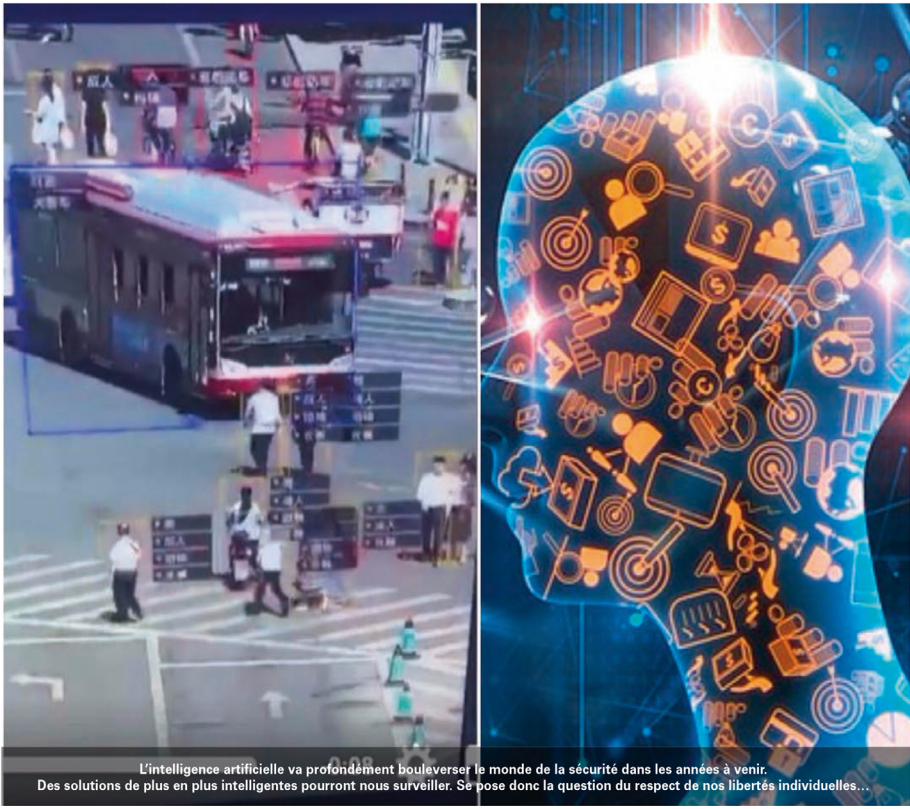
- Concrètement, l'IA, c'est quoi?
- L'IA est-elle dangereuse?
- Une vraie utilité
- D'autres marchés?
- Et l'homme dans tout ça?

**Article - L'IA AU SERVICE DE LA SÉCURITÉ**

PSM - N° 249 - Septembre/Octobre 2018



**dossier**



**L'IA: utile mais sous certaines conditions**

L'IA dans la sécurité n'est pas qu'une vue de l'esprit ou un outil marketing. Ses applications sont réelles et vont sans doute se généraliser. Mais cela ne doit pas empêcher tous les acteurs concernés de se poser la bonne question: l'IA, pour quoi faire?

**O**n en parle de plus en plus. Et le monde de la sécurité ne cesse de bruiser de ses possibles applications et des bouleversements qu'elle devrait engendrer tant du point de vue des solutions proposées que des services ou du rôle de l'homme dans la chaîne sécuritaire. Qui est ce «elle»? C'est l'IA ou «intelli-

gence artificielle» que d'aucuns définissent comme l'ensemble des techniques qui doivent permettre aux machines d'imiter une forme d'intelligence réelle. Et l'IA est aujourd'hui utilisée dans un nombre, toujours plus important, de domaines d'applications. La sécurité est évidemment l'un d'eux.

**Article - L'IA AU SERVICE DE LA SÉCURITÉ**

PSM - N° 249 - Septembre/Octobre 2018



**L'IA AU SERVICE DE LA SÉCURITÉ**

Mais sous cette apparente simplicité de la définition, on peut mettre de nombreuses choses. Et il ne faut pas croire que l'IA est si nouvelle qu'elle en a l'air. En effet, la notion d'IA apparaît dans les années cinquante grâce aux travaux du mathématicien Alan Turing dont le livre *Computing Machinery and Intelligence* pose déjà la question de la possibilité d'apporter aux machines une forme d'intelligence. Alan Turing va plus loin puisqu'il conçoit un test – le célèbre test de Turing – dans lequel un sujet interagit à l'aveugle avec un autre humain, puis avec une machine programmée pour formuler des réponses sensées. Si le sujet n'est pas capable de faire la différence, alors la machine a réussi le test et, selon Turing, peut être considérée comme « intelligente ».

■ **Concrètement, l'IA, c'est quoi ?**

L'acronyme IA signifie couramment intelligence artificielle, mais pour Vincent Le Cerf, docteur en intelligence artificielle il est plus juste de parler d'« informatique avancée ». Ce qui fait que la définition de l'IA évolue au fur et à mesure des avancées sur l'algorithmie.  
 « Si l'IA cherche à reproduire l'intelligence humaine, elle reste avant tout un ensemble de logiciels conçus pour réaliser des instructions prédéterminées. À l'heure actuelle, on est encore loin de reproduire le travail du cerveau humain qui est capable de sentir, d'analyser, d'interpréter et d'agir, en s'adaptant à son environnement. » note Vincent Le Cerf.  
 Pour Pascal Pech, directeur général solution sécurité chez Onet : « Le concept d'intelligence artificielle recouvre plusieurs technologies, c'est pourquoi il est parfois difficile de faire la part des choses entre des innovations structurantes pour le futur et des applications plus basiques. Les effets d'annonce ajoutent d'ailleurs à la confusion. Il est donc important de clarifier le ●●●



●●● *concept. Pour commencer, je dirais que l'intelligence artificielle recouvre aujourd'hui un ensemble de techniques, machine learning, computer vision, natural language processing qui sont utilisées pour de nombreuses applications, telles que le data mining, les chatbots et assistants virtuels, les capteurs intelligents ou*

*encore la robotique.» Mais il tient à préciser que « certaines techniques sont matures comme le natural language processing pour les chatbots, quand d'autres commencent juste à être utilisées – comme le deep learning – dans des applications limitées avec la reconnaissance de forme dans une photographie, par exemple. »*

## Article - L'IA AU SERVICE DE LA SÉCURITÉ

PSM - N° 249 - Septembre/Octobre 2018



### L'IA AU SERVICE DE LA SÉCURITÉ

#### ■ L'IA est-elle dangereuse ?

Parler de l'IA et de ses possibles applications ne doit pas nous interdire de nous poser certaines questions. Comme le souligne Genséric Cantournet, Pdg de Kelony : « L'IA n'est pas un sujet neutre dans la mesure où il ne laisse pas indifférent. L'IA est porteuse de craintes : accentuation du chômage, implications en matière de protection de la vie privée ou bien d'éthique, etc. Ces craintes sont le fruit d'un biais cognitif concernant la manière de percevoir et d'aborder aujourd'hui les enjeux de l'IA. Ce biais s'étend d'un extrême à l'autre : omnipotence thaumaturgique supposée d'un côté et surévaluation anthropomorphique de l'autre. Ces derniers sont supposément dus à des formes d'autonomisation potentielle hors d'un quelconque contrôle. En réalité, ces risques sont moins ceux de l'IA que ceux de sa conception par l'Homme. Ce biais n'est pas propre à l'IA, c'est celui d'une innovation galopante sans précédent. »

Cela posé, les enjeux de l'IA sont bien réels. En matière de développement et de problèmes d'application pratique opérationnelle. « Au premier rang desquels, celui de la gouvernance des modalités de contrôle sur l'évolution inférentielle des algorithmes et l'anticipation des risques systémiques. C'est en particulier prégnant pour les algorithmes auto-évolutifs à apprentissage rétroactif, capables d'apprendre à apprendre. Ces derniers sont capables d'apprendre à partir de leurs échecs et d'évoluer en mode "dégradé" le cas échéant. Les algorithmes de type Proximal Policy Optimization ou Hindsight Experience Replay permettent à la machine qui serait dans l'incapacité d'exécuter une tâche d'en choisir une autre en toute autonomie », ajoute le dirigeant de Kelony.

Cette question de l'autonomie de l'IA est aussi une de celles que se pose maître Alain Bensoussan, fondateur du cabinet Lexing Bensoussan Avocats et qui réfléchit depuis plusieurs années sur les questions de robotiques, d'intelligence artificielle, de responsabilité juridique des machines : « L'intelligence artificielle oblige les professionnels de sécurité, les pouvoirs publics et les utilisateurs de solutions à se poser des questions cruciales quant à notre rapport à la machine et sa capacité à décider à notre place. Nous sommes en effet aujourd'hui confrontés à des questions inédites en matière de responsabilité face à la généralisation de ces technologies ». Car, jusqu'à maintenant, la décision incombait à l'opérateur. Mais demain qu'en sera-t-il puisque désormais les machines et autres robots sont capables d'apprendre par eux-mêmes ? « Quid de leur capacité de résistance face à une atteinte, dans l'éventualité où, confrontés à des données fausses ou mal interprétées, ils seraient susceptibles de déclencher une action ou une réponse erronée face à un incident ? », s'inquiète donc Alain Bensoussan.

Vous avez peut-être vu le film américain *I-Robot* dans lequel un androïde, après analyse d'une situation dramatique – un homme et une petite fille sont en train de se noyer – décide de sauver l'homme car, après analyse froide, le robot juge que l'homme a plus de chances de survivre... Choix choquant ? Certes. Mais qui est responsable ? La machine ou l'ingénieur qui l'a programmée ? Les professionnels de la sécurité qui développent les outils que nous voyons se généraliser aujourd'hui, principalement dans la vidéosurveillance, ne se posent pas tous forcément encore ces questions. Ils vont pourtant devoir le faire, tout comme le législateur et les pouvoirs publics.

#### ■ Une vraie utilité

« L'intelligence artificielle est très intéressante pour le monde de la sécurité. Les capacités d'auto-apprentissage sont très utiles pour la reconnaissance faciale, par exemple. Mais cela requiert d'importantes bases de données comme celles dont disposent aujourd'hui Google ou Facebook. Il faudra aussi disposer d'outils qui permettront d'analyser ces bases de données. Comme le deep-face de Facebook qui conçoit le modèle qui lui permet de reconnaître les personnes. On peut d'ailleurs s'interroger sur l'avenir des bases de données des grandes sociétés de l'internet et des réseaux sociaux. Elles ne sont encore utilisées que par ces sociétés. Mais s'il leur prenait l'envie de les monétiser un jour ? Actuellement, les systèmes qui utilisent de l'IA fonctionnent soit à base de règles qui leur sont inculquées par l'humain afin de stimuler des raisonnements simples sur des données soit par des processus d'auto-apprentissage à partir de bases de données d'exemples. Ils sont alors capables d'analyser, corrélérer et déduire l'information afin de potentiellement décider », explique Marie-Claude Frasson, directrice technique chez Digital Barriers.

Pour que cela tourne cependant de manière correcte, il faut beaucoup de capacités CPU et des algorithmes puissants. On peut aussi imaginer que l'IA pourra être utilisée dans des applications de contrôle d'accès pour reconnaître la signature visuelle d'un individu afin de la comparer avec les signatures visuelles des individus contenus dans une base de données. L'IA peut aussi être appliquée pour identifier des "pattern of life", des comportements individuels qui se modifient sans raison apparente. Tout cela pose donc la question primordiale de la gestion des bases de données. Qui en dispose ? Comment sont-elles constituées ? Pour quelles utilisations ? Il faudra veiller à faire attention aux problématiques des libertés individuelles et publiques...

« L'IA ne sera utile que si elle nous permet de gagner du temps pour intervenir face à un délit, martèle Dominique Legrand, président de l'AN2V. Elle doit donc s'inscrire dans un contexte global pour permettre à l'opérateur d'agir en temps réel. C'est-à-dire, de détecter une anomalie grâce à des outils d'analyse vidéo et audio, de transmettre l'information et de l'analyser – 24 h/24 et 7 j/7 – pour permettre aux forces de l'ordre d'intervenir. C'est grâce à cet apport de l'IA que la sécurité privée pourra aussi s'inscrire dans le continuum de la sécurité tant souhaité par les pouvoirs publics et les acteurs privés du secteur. »

Mais pour arriver à cela, il faut anticiper la rupture technologique que représente l'IA. « Beaucoup de gens parlent de l'IA, surtout dans le monde de la vidéosurveillance, mais peu se sont réellement préparés au saut technologique qu'elle représente, regrette Laurent Scetbon, responsable d'équipe grands comptes et projets chez Hikvision. Se préparer à l'IA, comme nous l'avons fait puisque nous proposons déjà des solutions qui intègrent ces technologies, implique de gros investissements en matière de R&D pour concevoir des solutions que pourront réellement apporter une plus-value à l'opérateur derrière son écran. L'IA devra être capable d'apprendre et de reconnaître des cibles différentes et d'aider, a posteriori, à la recherche d'individus selon leur sexe, âge, vêtements, couleur de cheveux, lunettes, etc. »

**Article - L'IA AU SERVICE DE LA SÉCURITÉ**

PSM - N° 249 - Septembre/Octobre 2018



**L'IA AU SERVICE DE LA SÉCURITÉ**

La vidéosurveillance n'est pas le seul marché de la sécurité concerné par le développement de l'IA. Le contrôle d'accès y réfléchit aussi. « Avec l'IA, on peut raisonnablement envisager d'accroître les capacités des lecteurs de contrôle d'accès pour leur permettre de devenir de véritables capteurs à l'instar des caméras, souligne Vincent Dupart, Pdg de STid. En y intégrant des algorithmes, nous pourrions leur permettre d'identifier des comportements suspects (attitudes, gestes, reconnaissance faciale, port d'armes...), à l'entrée d'une banque par exemple. Par ailleurs, associer de l'IA à un drone - ce que nous faisons déjà avec notre partenaire Novadem - nous offre l'opportunité de proposer un autre type de contrôle d'accès et de gestion des flux sur un site. On peut identifier les personnes lorsqu'elles se déplacent sur une zone sensible, vérifier qu'elles ont le droit d'accéder à telle ou telle zone et éventuellement les interpeller en cas de non respect des droits d'accès... »

**■ D'autres marchés ?**

Il est indéniable que l'apport de l'IA dans les services, solutions et prestations de sécurité ouvre aux acteurs du marché de formidables opportunités en matière de développement d'activités et de diversification. « Bien entendu ces nouvelles technologies vont avant tout nous permettre d'améliorer la sécurité ● ● ●

● ● ● globale des sites, celle de nos agents et la performance économique de nos prestations, reconnaît Pascal Pech. Mais le couple homme/machine va aussi nous conduire à aborder la sécurité de manière différente, en proposant de nouveaux services et en adoptant de nouveaux business model. Chez Onet, le développement de l'IA nous permet d'envisager des synergies inter-activités : des données obtenues à partir des capteurs sécurité pourront par exemple se révéler utiles pour adapter nos prestations de nettoyage aux flux des usagers. Des solutions de smart cleaning sont d'ailleurs déjà en place sur plusieurs sites client. D'autres synergies sont possibles avec notre activité de logistique, comme des solutions de traçabilité mixte. L'interopérabilité entre nos métiers est un véritable axe de développement. »

Point de vue que partage Laurent Scetbon : « L'IA nous permet déjà et nous permettra encore plus de s'adresser à d'autres marchés comme le commerce de détail, la grande distribution ou le marketing afin de leur proposer des outils d'aide à la gestion des magasins, des stocks, des effectifs et de la clientèle. »

**■ Et l'homme dans tout ça ?**

Avec le développement des applications IA et leur généralisation se pose une question : va-t-on, comme le pensait le Pdg de Securitas, de manière un peu provocante certes, vers une sécurité sans homme, sans opérateur ? « Le marché est très demandeur mais il faut garder à l'esprit que, dans nos métiers, la machine ne remplacera jamais ni l'expérience, ni la pertinence de l'humain. Les compétences de nos opérateurs de télévidéosurveillance ou de nos agents de sécurité devront bien sûr évoluer pour leur permettre de mieux interagir avec l'ensemble de ces outils : analyser la donnée, manipuler un drone ou un robot nécessiteront d'adapter les formations. Mais notre conviction est que l'homme est incontournable dans le domaine de la sécurité, et nous misons sur ce couple homme/machine plus que sur des systèmes autonomes », tient à rappeler le directeur d'Onet Sécurité.

La robotique et les drones sont évidemment un des axes de travail majeur en matière d'IA dans la sécurité. « Dans nos drones, nous mettons de l'IA pour que la machine soit capable de présenter à un opérateur qualifié une information crédible et utile, explique Grégoire Linard, directeur R&D d'Azur Drones, leader européen du drone de surveillance. Notre but n'est pas de remplacer l'homme, mais de lui permettre, grâce à l'apport de l'IA, de se concentrer sur des tâches plus valorisantes, tout en ne l'exposant pas inutilement à certains risques. L'IA nous permet d'effectuer automatiquement de la levée de doute et des rondes automatiques mais pas uniquement. Nos drones sont capables aussi de modéliser un site afin de faciliter, par exemple, l'accès à certaines zones en cas d'incident ou les déplacements des secours pour éviter qu'ils soient contraints de traverser une zone dangereuse ou interdite. L'IA au service de l'homme et de sa sécurité... » ■

