Vol. 30, n° 3

Gagner la guerre du futur : considérations juridiques et éthiques sur l'intelligence artificielle

Anne Cammilleri*

* Professeure des Universités, Université Paris 13-Sorbonne Paris Cité, codirectrice du Master Sécurité Défense et Intelligence Stratégique, Sciences Po Rennes. Cet article résulte d'une conférence réalisée à l'Université Laval. Tous mes remerciements à l'Université Laval et tout particulièrement au Centre sur la sécurité internationale des Hautes études internationales et à l'Institut militaire de Québec pour leur invitation à ce colloque sur le sujet de la guerre du futur. Mes remerciements vont aussi à Stéphane Lemaan-Langlois, titulaire de la chaire sur la surveillance et la construction sociale du risque, à la rectrice de l'Université Laval, Sophie D'Amours, au brigadier-chef général Richard Giguère, et à Pierre Colautti.
[Note : cet article a été soumis à une évaluation à double anonymat.]

RÉSUMÉ

Afin de gagner la guerre du futur, il faut désormais penser une stratégie globale de cybersécurité dans le cyberespace, stratégie qui se construit sur nos valeurs et le renforcement de la protection des droits fondamentaux.

MOTS-CLÉS

cyberespace ; droit comparé ; intelligence artificielle ; personnalité ; vie privée ; moyens techniques de protection

INTRODUCTION

La guerre du futur se joue aussi désormais dans le cyberespace que certains aimeraient voir comme un territoire sans foi ni loi. Or rien de tel ! Le progrès scientifique réalisé par les chercheurs dans le monde entier contribue à nous faire entrer dans un nouvel espace où l'intelligence artificielle nous oblige déjà à réfléchir aux règles fondamentales – éthiques et juridiques – que nous souhaitons défendre pour construire la paix des générations à venir alors que se joue déjà la guerre du futur.

Il s'agit bien d'une guerre larvée, car l'ennemi n'est plus toujours physiquement en face, clairement identifié ; la guerre n'est même pas déclarée. Ses menaces comme ses attaques sont à la fois ciblées et multidimensionnelles. Mais, face à cette révolution plutôt récente, les États ont établi des stratégies claires, cumulatives d'anticipation des cybermenaces par la cyberdéfense et de répression de la cybercriminalité par l'incrimination pénale au nom de la protection de la souveraineté nationale. La guerre du futur – qui est déjà celle d'aujourd'hui – nous impose de repenser nos fondamentaux : il faut désormais penser une stratégie globale de cybersécurité dans le cyberespace. Une stratégie qui se construit sur nos valeurs et sur le renforcement de la protection des droits fondamentaux : nous faisons la guerre […] pour la gagner sur la base de nos valeurs.

1. ÊTRE AGILE POUR GAGNER LA GUERRE DU FUTUR

Les vainqueurs de cette cyberguerre seront les États qui auront su être agiles dans la construction de leur stratégie (1.1) et qui auront construit un système de droit adaptable à la polymorphie des menaces (1.2).

1.1 L'agilité

Cette agilité se doit d'être institutionnelle (1.1.1) et matérielle (1.1.2).

1.1.1 L'agilité institutionnelle

L'agilité institutionnelle ou organique se traduit, dans nos systèmes de droit, par notre capacité rapide à passer d'un système de cybersécurité défensif à une capacité de réaction offensive. Cette démarche s'est effectuée dans un temps court pendant lequel les États ont renforcé leur organisation. Pour ce faire, il a fallu identifier les principaux acteurs régaliens. Pour ne prendre que deux exemples : la France, via le Secrétariat général de la sécurité et de la défense nationale (SGDSN), directement rattaché au service du premier ministre, a créé une catégorie d'acteurs particuliers, les Organismes d'importance vitale (OIV), ayant permis d'identifier 16 secteurs d'activités particulièrement sensibles. Cette identification des secteurs s'est accompagnée de la montée en puissance d'un acteur, au sein du SGDSN, soit l'Agence nationale de sécurité des systèmes d'information (ANSSI)[1] dont les compétences ne cessent de croître, pour s'adapter au plurimorphisme des menaces au sein du cyberespace.

Le Canada développe la même agilité avec une stratégie clairement identifiée afin de renforcer la projection des « infrastructures essentielles » protégeant quasiment les mêmes secteurs régaliens ou industriels (l'énergie, les finances, l'alimentation, les TICE, le transport, la santé, la sécurité, l'eau, l'armement et l'industrie). La France y ajoute, sans surprise, depuis le 1er avril 2017, les activités nucléaires et spatiales.

Mais l'agrégation institutionnelle des forces repose sur l'agilité des autres institutions régaliennes à dialoguer sur la base de la stratégie de cybersécurité qui est clairement posée en France en 2009 et dès 2010 au Canada.

Au Canada, Sécurité publique Canada et en France le SGDSN coordonnent la mise en œuvre de la stratégie de la cyberdéfense : le Centre de sécurité des télécommunications au Canada et l'ANSSI en France ont un rôle semblable d'expertise et de détection. Dans ces deux États, afin d'évaluer la menace interne et étrangère, les actions s'intensifient et s'appuient sur le service canadien de renseignements et en France sur la Direction générale de la sécurité intérieure, la

1. Décret nº 2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information », modifié par le décret nº 2015-351 du 27 mars 2015 relatif à la sécurité des systèmes d'information des opérateurs d'importance vitale et pris pour l'application de la section 2 du chapitre II du titre III du livre III de la première partie de la partie législative du code de la défense.

Direction générale de la sécurité extérieure et la Direction du renseignement militaire.

Dans ces deux États encore, les gendarmes ont un rôle d'enquête cybercriminelle en lien étroit avec Europol et Interpol qui permet de lier les notions de sécurité intérieure et extérieure.

Les ministres responsables de la défense ou des affaires étrangères, dans le cadre des partenariats onusiens et européens, contribuent, ensemble, au renforcement de la résilience des forces pour mener à bien les opérations extérieures se déroulant aussi dans le cyberespace.

Enfin, le nerf de la guerre étant aussi financier, les ministres responsables des finances agissent conjointement dans le cadre de la lutte contre le terrorisme (p. ex. : l'ANSSI en charge de mieux contrôler la sécurité de l'autorité des marchés financiers en 2018). Ce dialogue national et international a permis aux deux États de passer d'une posture nationale défensive à une posture internationale offensive, sans toutefois avoir la force de frappe financière des États-Unis d'Amérique. Depuis 2011, on peut dire que la cyberguerre du futur sera clairement défensive, mais surtout offensive. Nous agissons chaque fois que nos intérêts sont en danger, tout en restant dans une posture internationale défensive, afin de respecter les traités internationaux. Nous sommes devenus agiles… car proactifs. Le monde cyber nous appartiendrait-il ?

En France, pour rendre cette agilité effective, la *Loi de programmation militaire* (LPM)[2] couvrant la période 2019-2025 permet un sérieux renforcement de cette cyber-résilience : l'objectif présidentiel affiché est un budget de la défense à 2 % PIB en 2025 avec un budget moyen annuel de 39,6 milliards par an (2018 : 34,2 milliards). On y soulignera la montée en puissance, initiée en 2015, du Comcyber effectivement créé en 2016[3], commandé par le général Olivier Bonnet de Paillerets qui assume la dimension défensive française (avec en 2017, dix incidents graves dont cinq jugés critiques)[4], mais

2. Projet de loi relatif à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense, NOR : ARMX1800503L/Bleue-1, France, Ministère des armées, en ligne : <https://www.defense.gouv.fr/portail/enjeux2/la-lpm-2019-2025/le-projet-de-loi/loi-de-programmation-militaire-2019-2025-textes-officiels>.
3. Décret n° 2017-743 du 4 mai 2017 relatif aux attributions du chef d'état-major des armées, JORF du 5 mai 2017 ; Arrêté du 4 mai 2017 modifiant l'organisation de l'état-major des armées, JORF n° 0106 du 5 mai 2017.
4. Audition du général Olivier de Pailleret sur la loi de programmation militaire, le 17 mars 2018 devant la Commission de la Défense Nationale et des forces Armées

surtout l'offensive en Syrie contre Daech, par notamment des actions de contre-propagande. L'objectif affiché de la LPM est de 2600 combattants numériques en 2019 auxquels il convient d'ores et déjà d'ajouter les 600 experts de la Délégation générale pour l'armement du ministère des armées, les 400 réservistes opérationnels et les 4000 réservistes citoyens de la cyberdéfense. Cette restructuration du ministère des armées autour du Comcyber permet notamment de mieux caractériser la menace et d'agir de manière plus ciblée. Il a permis de renforcer le système d'information des armées en intégrant l'intelligence artificielle et le *big data*.

On soulignera également que l'article 19 de la LPM ainsi que la loi du 26 février 2018, transposant la directive NIS[5], renforcent considérablement les pouvoirs de l'ANSSI, lui permettant d'intervenir dès lors qu'elle a connaissance d'une menace susceptible de porter atteinte à la sécurité des réseaux des systèmes d'information des autorités publiques ou des opérateurs en s'appuyant sur le réseau d'un opérateur de communications électroniques, y compris sur le système d'information d'une personne. Il en est de même de la création d'un système de détection recourant à des marqueurs techniques à la seule fin de détecter des événements susceptibles d'affecter la sécurité des systèmes d'information. Cette mise en œuvre pour la durée et dans la mesure strictement nécessaire à la caractérisation de la menace est un objectif clairement offensif au service de la cyber-résilience. On est ainsi très loin de la pensée d'une indépendance dans le cyberespace telle que défendue par feu John Perry Barlow. Il n'y a d'indépendance dans le cyberespace que si l'État se montre capable d'agilité technologique. Agilité technologique certes, mais qui ne semble pas toujours très respectueuse de la protection des droits fondamentaux. La réserve d'exigence fondamentale semble ici s'effacer dans la guerre du futur.

---

de l'Assemblée nationale, compte rendu n° 41 qui mentionne notamment « les exigences d'adaptation à l'innovation qui passe par la modernisation des équipements, mais aussi de l'expertise technique, technologique et la capacité analytique pour les enquêtes sur les réseaux ». Il mentionne également l'exigence d'un modèle solide et agile pour le combat numérique, « hyperconnexion exige que le défi de la cyber-résilience soit relevé dès maintenant » (Déclaration au Forum international de la Cybersécurité, *Revue de la Gendarmerie Nationale*, Centre de recherche de l'École des Officiers de la Gendarmerie Nationale (CREOGN), 2018, en ligne : <https://www.gendarmerie.interieur.gouv.fr/crgn/Publications/Revue-de-la-gendarmerie-nationale>).

5. Loi n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité, JORF n° 0048 du 27 février 2018 ; Directive 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant les mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union, JOUE L 194 du 19 juillet 2016.

L'agilité organique de la France et du Canada se fonde, en dernier lieu, sur le renforcement du dialogue interinstitutionnel dans le cadre de l'Union européenne grâce à l'accord de partenariat stratégique[6], mais aussi grâce à celui, plus récent, sur les échanges concernant les informations classifiées[7].

1.1.2 L'agilité matérielle

Tous les acteurs européens et internationaux sont à l'œuvre pour favoriser l'agilité matérielle dans le cyberespace. À titre d'exemple, en France, le rapport Villani[8] prend en considération cette exigence d'agilité au regard de la protection de l'information classifiée et il souligne la nécessité de repenser les mécanismes de déclassification de l'information automatisée, de la nécessité de penser à la définition d'une date de péremption de la classification ou encore d'engager une réflexion sur l'évolution de la classification de la sensibilité d'une donnée.

L'Union européenne devient proactive dans le cyberespace en promouvant un niveau élevé commun de sécurité des réseaux. Rappelons quelques événements cruciaux de l'année : depuis le 10 mai 2018, la *Directive NIS du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux*[9], s'appuyant sur la *Directive du 2008/114/CE du 8 décembre 2008 concernant le recensement des infrastructures critiques européennes*[10], doit être transposée dans tous les États membres. Ce nouveau cadre normatif va permettre une vraie révolution culturelle, notamment par l'obliga-

---

6. Accord de partenariat stratégique entre l'Union européenne et le Canada du 30 octobre 2016.
7. Décision (PESC) 2017/2322 du Conseil du 29 mai 2017 relative à la signature et à la conclusion de l'accord entre le Canada et l'Union européenne sur les procédures de sécurité pour l'échange d'informations classifiées et leur protection et l'Accord entre le Canada et l'Union européenne sur les procédures de sécurité pour l'échange et la protection d'informations classifiées, JOUE L 333 du 15 décembre 2017.
8. Cédric VILLANI, Marc SCHOENAUER, Yann BONNET, Charly BERTHET, Anne-Charlotte CORNUT, François LEVIN et Bertrand RONDEPIERRE, « Donner un sens à l'intelligence artificielle : pour une stratégie nationale et européenne », France, mission confiée par le premier ministre Édouard Philippe, en ligne : <https://www.aiforhumanity.fr/pdfs/9782111457089_Rapport_Villani_accessible.pdf>.
9. Directive 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant les mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union, JOUE L 194 du 19 juillet 2016.
10. Directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection, L 345/75 du 23 décembre 2008.

tion de décloisonner les règles de cyberattaques grâce à la création du Réseau de centres de réponses aux incidents de sécurité informatique (CSIRT) ; la promotion d'une coopération opérationnelle, effective, rapide et le renforcement de la coopération internationale (accords internationaux *ad hoc*) sont autant d'éléments qui font de l'Union européenne une actrice non négligeable du cyberespace. Chaque État membre doit prévoir une obligation de notification des incidents et à défaut – à titre d'exemple – en France, des sanctions pécuniaires substantielles allant de 50 à 100 000 euros sont prévues par la loi. Cette notification obligatoire est circonscrite aux incidents ayant eu un impact significatif sur la continuité des services essentiels, mais ne concerne pas les petites entreprises. Le législateur européen prévoit également la notification volontaire d'incidents aux autres entités.

La normalisation de la sécurité des réseaux des Systèmes de sécurité d'information via l'Agence Européenne chargée de la sécurité des réseaux et de l'information (ENISA) doit se lire en lien étroit avec la proposition de règlement du Parlement européen et du Conseil du 4 octobre 2017 qui vise également la définition de bonnes pratiques de résilience dans le cyberespace[11] et à faire émerger une culture de l'anticipation. L'objectif recherché est que l'ENISA ne soit plus une simple agence opérationnelle, mais devienne une agence de services, notamment avec un rôle déterminant en matière de certification européenne. Les discussions actuelles sur le texte au niveau européen évoluent vers la consécration d'une compétence partagée de l'Agence avec le Groupe européen de certification de la cybersécurité et la Commission européenne[12].

Enfin, on peut se référer à l'entrée en vigueur de *l'Accord entre l'UE et l'Australie* à durée indéterminée du 15 septembre 2017[13] dont l'article 11 relatif « à la sécurité internationale et le cyberespace » démontre que les États membres de l'Union et l'Australie accordent une importance certaine à la coopération et les échanges de vues. Le

11. Proposition de règlement du Parlement européen et du Conseil du 4 octobre 2017 relatif à l'ENISA, Agence de l'Union européenne pour la cybersécurité, et abrogeant le règlement (UE) nº 526/2013, et relatif à la certification des technologies de l'information et des communications en matière de cybersécurité (règlement sur la cybersécurité, COM(2017) 477 Final) ; Anne CAMMILLERI, « Droit de la cybersécurité et intelligence artificielle, le rejet de la "singularité technologique" », *Chronique annuelle sur les nouvelles technologies*, RDUE 2017, nº 4, p. 99-143.
12. Seconde lecture au Parlement européen le 27 mars 2018, *Accroître la transparence et la confiance et la sécurité des TIC*.
13. Accord UE/Australie à durée indéterminée du 15 septembre 2017 sur décision du Conseil du 29 décembre 2016. Partie II de l'accord-cadre entre l'Union européenne et ses États membres, d'une part, et l'Australie, d'autre part, JOUE L 237 du 15 septembre 2017, p. 7-35.

domaine de la sécurité internationale et le cyberespace sont au cœur de cet accord, les parties ayant pour objectif commun la lutte contre la cybercriminalité (art. 36 de l'accord)[14], mais aussi la protection du renseignement de la défense et des affaires militaires (art. 60 de l'accord).

Au niveau de l'OTAN, on soulignera la grande adaptabilité et l'agilité que développe l'organisation depuis le Sommet de Chicago. L'agilité et l'interopérabilité vont de concert dans toutes les conclusions officielles des réunions du Conseil. L'attention est toute particulière lors du Sommet du Pays de Galles en 2014, où les chefs d'État ou de gouvernement ont entériné une « politique de cyberdéfense renforcée » pouvant s'appuyer sur le recours à l'article 5 du traité otanien pour qualifier une cyberattaque d'agression armée dans le cyberespace et permettant ainsi une action de légitime défense[15].

Notons toutefois, en dernier lieu, que cette agilité organique et matérielle s'inscrit dans le plein respect de la souveraineté des États. À ce titre, il n'est pas anodin de souligner que la gestion des secrets n'est pas un frein. En effet, tous les États invoquent la protection de leurs intérêts essentiels pour identifier ce qui ressort de la coopération internationale de ce qui relève de l'essence même du secret de l'État souverain[16]. Il en est de même de la Loi canadienne sur les secrets officiels[17] de 1939, révisée en 1973 en faveur des écoutes téléphoniques sur autorisation du pouvoir exécutif (et non juridictionnel).

Cette agilité permet d'adapter nos systèmes normatifs au service de la défense de nos valeurs démocratiques (1.2).

1.2 L'adaptabilité de nos systèmes normatifs au regard des valeurs et de l'exigence de protection des droits fondamentaux

Cette adaptabilité est normative (1.2.1) et politique (1.2.2).

---

14. L'article 36 permet de renforcer les échanges d'informations et d'expériences concrètes relatifs aux domaines de la haute technologie du cyberespace, de l'électronique et la diffusion des contenus illégaux notamment terroristes sur l'Internet. Il étend la coopération également au domaine de l'éducation, la formation d'enquêteurs spécialisés dans la cybercriminalité et la criminalité numérique. Il est à noter que l'accord promeut la convention de Budapest sur la cybercriminalité « en tant que norme mondiale en matière de lutte contre la cybercriminalité ».
15. §72 de la Déclaration de l'OTAN lors du Sommet de Galles, 2014.
16. Rapport sur le secret de la défense nationale, janvier 2018 et la revue stratégique de la cyberdéfense du 12 février 2018 publié sur le site du SGDSN, en ligne : <http://www.sgdsn.gouv.fr>.
17. *Loi antiterroriste*, L.C. 2001, ch. 41, PARTIE 2 : LOI SUR LES SECRETS OFFICIELS, L.R., ch. O-5.

1.2.1 L'adaptabilité normative par la pénalisation de l'infraction dans le cyberespace européen

Pour gagner la guerre du futur dans le cyberespace, il faut considérer que ce dernier épouse les frontières des États. Cela permet d'imposer un critère de territorialité de l'infraction d'où pourra découler une sanction. Malheureusement, en Europe et ailleurs dans le monde, on assiste à l'émergence d'un lien prégnant entre la cybercriminalité et le terrorisme. En témoignent aussi les discussions canadiennes autour de l'adoption de la loi antiterroriste du 20 juin 2017 qui résultait de la nécessité d'adapter le droit pour définir cinq types d'incriminations dans le *Code criminel* (art. 320-1)[18]. Quelques mois auparavant, l'Union européenne adoptait une directive qui définissait la liste des actions terroristes devant être qualifiées d'infractions pénales[19]. À ces actions correspondent une dizaine d'infractions pénales intégrant des mesures minimales de sanctions. Cette directive devra être transposée avant le 8 septembre 2018 au sein des 27 États membres. Dans une France encore meurtrie par des attentats terroristes, la loi du 30 octobre 2017 en est l'écho anticipé[20].

L'effectivité de la sanction pénale ne suffit plus. Le juge européen, dans le cadre de l'examen des procédures d'enquête qui suivirent l'attentat de Londres en 2005, a rendu une série d'arrêts qui imposent le critère de l'existence d'une « enquête adéquate ». Ainsi, au nom de la protection du droit à la vie, la Cour européenne des droits de l'homme (CEDH) exige une obligation de rendre compte *a posteriori*. Pour ce faire, il convient d'apporter la preuve au juge que les représentants de l'État ont effectué une « enquête adéquate » pour démontrer que le recours à la force fut légitime, justifiant une atteinte à la vie[21]. Par ailleurs, l'effectivité de l'enquête doit être prouvée par des moyens démontrant que les personnes étaient indépendantes, sans lien hiérarchique avec l'autorité publique concernée et qu'il existait une indépendance concrète et effective de l'enquêteur. La CEDH va

18. L'article 320-1 *Code criminel* les définit comme le fait de participer, contribuer, faciliter une activité terroriste ; perpétrer une action grave au nom du terrorisme ; charger sciemment une personne de se livrer à une activité terroriste et l'existence d'une intention précise doit être établie. (*Code criminel*, L.R.C. 1985, ch. C-46).
19. Il s'agit de participer à une association ou groupe à des fins de terrorisme ; se rendre à l'étranger à des fins de terrorisme ; de financer des voyages à l'étranger à des fins de terrorisme ou encore d'organiser ou faciliter de quelque manière que ce soit des voyages à des fins de terrorisme. Directive (UE) 2017/541 du Parlement européen et du Conseil du 15 mars 2017 relative à la lutte contre le terrorisme et remplaçant la décision-cadre 2002/475/JAI du Conseil et modifiant la décision 2005/671/JAI du Conseil JOUE L 88, 31 mars 2017, p. 6-21.
20. Loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme, JORF n° 0255 du 31 octobre 2017.
21. CEDH, Gde Chb, 30 mars 2016, Armani Da silva/ Roy. Uni.

examiner par ailleurs si les autorités avaient effectivement pris des mesures raisonnables pour l'obtention des preuves. Si tel est bien le cas, les conclusions de l'enquête doivent s'appuyer sur une analyse « méticuleuse, objective et impartiale ». À cela s'ajoute le contrôle par la Cour de l'effectivité de l'exigence de célérité et de diligence implicite de l'enquête. On assiste ainsi en Europe à un haut niveau d'exigence du standard de protection du droit à la vie, cette exigence même qui devra être reprise dans les enquêtes pénales de cybercriminalité. Cette jurisprudence n'est pas si étrangère aux Canadiens comme l'a explicité le général Raymond Hénault lorsqu'il évoquait « les idéaux canadiens »[22] dans la guerre du futur. Il résulte de la jurisprudence européenne cette chose précieuse selon laquelle la guerre du futur devra s'adapter à cette exigence fondamentale… de protéger la vie.

1.2.2 L'adaptabilité politique dans l'Union européenne : vers une défense européenne commune ?

En Europe, la constitution de la coopération structurée permanente est-elle un vrai événement politique signalant une nouvelle capacité d'agilité politique ? La décision posant les règles de sa création est à coup sûr un signal politique fort de la volonté de l'Union européenne de s'adapter à la guerre du futur. Créée sur la double base juridique de l'article 42§6 du *Traité sur l'Union européenne* et de son protocole n° 10, la décision du Conseil du 11 décembre 2017[23] en a défini les contours. Alors que les coopérations renforcées sont conditionnées par le regroupement de neuf États au minimum, le mouvement politique européen en faveur de la relance de l'Union européenne a touché la belle au bois dormant qu'était la coopération structurée permanente pour réussir cet exploit de réunir 25 des 27 États membres. En effet, seul le Royaume-Uni, pour les raisons de l'ouverture des négociations de sortie de l'Union européenne, le Danemark, par le recours au protocole *ad hoc* au *Traité de Lisbonne*[24] qui le délie de ses obligations relatives à la Politique de sécurité et

22. Propos d'ouverture du colloque pour la 9e rencontre internationale Université-défense de Québec du général (ret) Raymond Hénaut, membre du comité consultatif ministériel pour l'examen de la politique de défense et ancien Chef d'État major de la Défense du Canada, UNIDEF 9, *La guerre du futur*, Université Laval, 1er mars 2018.
23. Décision (PESC) 2017/2315 du Conseil du 11 décembre 2017 établissant une coopération structurée permanente (CSP) et fixant la liste des États membres participants, JOUE L 331/57 du 14 décembre 2017 ; décision (PESC) 2018/340 du Conseil du 6 mars 2018 établissant la liste des projets à mettre sur pied dans le cadre de la CSP, JOUE L 65, 8 mars 2018, p. 24-27.
24. Versions consolidées du Traité sur l'Union européenne et du Traité sur le fonctionnement de l'Union européenne, *Journal officiel de l'Union européenne*, n° C 326 du 26/10/2012, p. 1-390.

de défense commune (PSDC), et Malte, au regard de sa difficulté à remplir les critères élevés de capacités requises, ne sont pas parties à la coopération. Au-delà de l'exploit politique de la création de la coopération structurée permanente, il va s'agir désormais de la faire vivre. L'organisation qui ressort du texte juridique signifie clairement le retrait de l'Agence européenne de défense – qui tout en « soutenant la coopération » par l'évaluation des contributions des États participants et « en facilitant et coordonnant » les projets de développement des capacités – voit son rôle stratégique bien peu mis à l'honneur en étant le simple « forum européen pour le développement des capacités européennes », alors que l'Organisation conjointe de coopération en matière d'armement (OCCAR) est qualifiée « d'organisme privilégié pour la gestion des programmes en commun »[25]. Au-delà de ce toilettage sévère de l'agence, la coopération structurée permanente permet aux États participants de définir un objectif ambitieux de maintien de la paix : « par la disponibilité, l'interopérabilité, la flexibilité et la capacité de déploiement des forces au regard des objectifs communs ». Mais, pour ce faire, les membres de la CSP adhèrent à l'exigence de normes communes techniques et opérationnelles garantissant l'interopérabilité avec l'OTAN. À défaut d'une réelle solidarité européenne, l'achat sur étagères américaines est ainsi presque juridiquement joué ! Mais il convient de retenir que cet écueil résulte moins de la capacité d'innovation d'un État[26] que de l'échec de la mise en œuvre des règles de solidarité européenne.

2. L'EXIGENCE DE FONDAMENTALITÉ DES DROITS DE L'HOMME DANS LA GUERRE DU FUTUR

Cette exigence traduit l'urgence de maintenir l'humain – la personne – au centre du dispositif décisionnel de la guerre du futur (2.1) et nous oblige à nous interroger sur les contours des règles éthiques à adopter dans le cadre du développement de l'intelligence artificielle dans la guerre du futur (2.2).

2.1 Maintenir la personne humaine au centre du dispositif décisionnel des guerres du futur

Le progrès scientifique va bénéficier aux guerres de demain. La robotisation déshumanise les champs de bataille. Quelle place doit-

25. Anne CAMMILLERI, « Recherche commun désespérément ! », *Blog droit européen d'Olivia Tambou*, avril 2018, en ligne : <https://blogdroiteuropeen.com>.
26. Éric FOURNIER, *Présentation du programme de recherche canadien IDEeS*, ministère de la Défense nationale et les Forces armées canadiennes, colloque UNIDEF 9, *La guerre du futur*, Université Laval, 1er mars 2018.

on accorder aux robots dotés d'une intelligence artificielle dans nos sociétés ? Faut-il s'inquiéter de la place croissante qu'ils occupent ? Faut-il leur accorder la personnalité juridique au même titre qu'une personne physique afin de régler les problèmes juridiques liés à leur intervention ? L'Union européenne s'interroge actuellement sur la base de l'article 114 du *Traité sur le fonctionnement de l'Union européenne*[27] sur l'ensemble de ces questions.

2.1.1 Caractérisation de l'intelligence du robot

Comme l'a démontré Jean-Gabriel Ganascia, l'intelligence du robot s'évalue sur la base de quatre caractéristiques : « 1. Sa capacité d'acquisition, d'autonomie pour une interconnectivité ; 2. Sa capacité d'apprentissage par l'expérience et l'interaction ; 3. La forme de l'enveloppe physique du robot ; et enfin 4. La capacité d'adaptation de son comportement et de ses actes à son environnement ». Nous nous placerons d'emblée sur le rejet de la théorie de la singularité technologique qui surpasse l'intelligence humaine et ferait perdre le contrôle de la machine par l'être humain[28]. Cette singularité technologique est portée par les GAFAM qui financent de très importants laboratoires de recherche universitaires pour asseoir leur légitimité agissant ainsi en « pompiers pyromanes »[29]. Ganascia soutient que la loi de Moore n'est pas une loi d'évolution et il existe une incapacité du robot à atteindre une intelligence forte. Ces conclusions sont en phase avec les travaux de l'Office parlementaire d'évaluation de choix scientifiques et technologiques français et ceux du Parlement européen. Plusieurs scientifiques ne cessent de rappeler « qu'un robot n'est qu'une machine qui bouge ». Laumond souligne ainsi « qu'un robot qui prend une décision hors de son milieu est une machine qui est tombée en panne ! »[30]. Pourtant, le courant en faveur de cette consécration de la personnalité juridique du robot prend de l'ampleur à coup de milliers de dollars de communication. Il soutient l'existence d'une classification des robots, mais sur quels critères ? Selon les porteurs de cette pensée, l'idée de leur attribuer un numéro d'immatriculation et une assurance obligatoire concourt à renforcer la sécurité juridique et financière des dommages éventuels causés. Mais quels seraient les cri-

27. Versions consolidées du Traité sur l'Union européenne et du Traité sur le fonctionnement de l'Union européenne, *Journal officiel de l'Union européenne*, nº C 326 du 26/10/2012, p. 1-390.
28. Lire en ce sens les travaux de Jean-Gabriel GANASCIA, *Le mythe de la singularité*, Paris, Seuil, 2017.
29. *Ibid*.
30. Jean-Paul LAUMOND, LAAS-CNRS, *La robotique : la fabrique du mouvement*, colloque CNAM, 2016, dans Valérie DEPADT et Didier GUEVEL (dir.), « La fabrique du robot humanoïde », *Lex Robotica*, LGDJ, Lextenso, mai 2018, p. 39-44.

tères de classification des robots ? Le recours à l'assurance obligatoire et à la constitution d'un fonds de compensation par le fabricant et le programmateur réglerait économiquement la question de la réparation du dommage. On pourrait ainsi créer un droit d'action du robot. Le sens humain ici est balayé en faveur d'une approche financière intéressée allant vers un droit à la réparation des dommages causés par le robot. L'Union européenne, à cette heure, rejette ce positionnement et a fait le choix de s'ancrer dans la modernité en se saisissant de cette révolution industrielle majeure pour anticiper ce nouveau monde du numérique et de l'intelligence artificielle. Travaillant sur la nécessité de renforcer l'interopérabilité, les champs de compétence de l'Union qui semblent à cette heure privilégiés sont la politique des transports, la politique spatiale, l'éducation et l'emploi, la santé et la protection de l'environnement (agriculture). Dans tous les secteurs où l'arrivée de l'IA serait un gain pour la société, dans ses dimensions économique, sociale et environnementale, le Parlement européen et la Commission semblent bien avoir une même acceptation du rejet de principe de la singularité technologique et œuvrent en faveur de mesures qui assurent le maintien de la personne humaine au cœur du dispositif décisionnel.

2.1.2 La méthode de l'Union européenne

Pour appréhender l'arrivée de l'IA, l'Union européenne fondera son action sur des principes juridiques et éthiques. L'intelligence artificielle est « un ensemble de notions s'inspirant de la cognition humaine ou du cerveau biologique et destiné à assister ou suppléer l'individu dans le traitement des informations massives »[31]. Il en résulte que les principes juridiques pris en considération sont ceux qui intègrent l'humain au cœur du centre de décision. La personne humaine va pouvoir s'appuyer sur les principes et les valeurs de l'Union, tels qu'ils sont définis dans les traités européens comme le respect de la dignité humaine, la protection de la vie privée dès la conception (*privacy by design*), la protection de la vie familiale, la protection de la propriété intellectuelle, le respect de la liberté d'expression et d'information, les principes de solidarité, de justice et de proportionnalité. Devrait émerger également un principe d'éthique *by design*. L'Union européenne pourrait créer une coopération renforcée réunissant au minimum neuf des 27 États membres pour poser les fondements d'une agence européenne d'enregistrement chargée de la robotique et de l'IA comme le préconise le rapport Villani en France. Cette option ne réglerait pas tous les problèmes, car elle cautionnerait

31. Cédric VILLANI, *supra*, note 8.

de facto « le fossé technologique entre les États membres », mais aussi ferait fi de la solidarité européenne. Aussi, l'option européenne qui semble à cette heure privilégiée serait le renforcement de l'ENISA au sein de l'Union européenne[32]. Au niveau français, une proposition de mettre en place un observatoire sur la non-prolifération des armes autonomes est une des pistes en cours de discussion.

Au titre des principes éthiques, l'Union européenne s'empare du début éthique en l'ancrant dans la charte des droits fondamentaux de l'UE. On assiste donc à une juridicisation des principes éthiques. La guerre du futur n'est pas exempte du respect de cette exigence fondamentale. De manière autonome, des discussions ont également lieu sur le recours au principe de précaution, mais un courant majoritaire semble vouloir le rejeter au motif qu'il briderait l'innovation dans la recherche. Dès lors, les auteurs du rapport Villani semblent soutenir le principe du « test de la qualité » comme facteur d'aide à la décision. Les principes éthiques retenus devront permettre d'encadrer la conception, la fabrication, l'essai, l'utilisation du robot, afin de démontrer que l'invention constitue une réelle amélioration de la vie humaine. Le recours à la définition d'un cadre éthique, dès la conception, doit permettre une « appréciation bienfaisante et non malveillante »[33], ce qui signifie que l'on s'inscrit dans la logique selon laquelle « l'IA est complémentaire à l'homme et ne la concurrence pas »[34]. C'est ce qu'Axel Kahn, médecin généticien, signifie lorsqu'il considère que « le génie humain survivra à l'intelligence artificielle »[35].

2.2 Quelle éthique pour l'IA au service de la guerre du futur ?

Comme l'a écrit Ganascia, « sans âme il n'y a pas d'intentionnalité propre ». Le robot n'ayant pas d'âme, cela implique le rejet de la singularité technologique. S'il convient de consacrer un principe d'éthique *by design*, il faut le faire avec prudence (2.2.1) en tenant compte de la nécessité de la compléter par d'autres principes (2.2.2).

32. Proposition de règlement du Parlement européen et du Conseil du 4 octobre 2017 relatif à l'ENISA, *supra*, note 11.
33. Cédric VILLANI, « La concurrence entre l'homme et l'IA n'a pas vraiment de sens », *L'hebdo*, nº 11, en ligne : <https://le1hebdo.fr/journal/numero/187>.
34. Cédric VILLANI, *supra*, note 8.
35. « Le génie humain survivra à l'intelligence artificielle », Axel KAHN interviewé par Hervé Nathan, *Journal Marianne*, 1er février 2018.

2.2.1 La prudence requise pour le recours à « l'éthique by design »

Il convient de s'interroger dès lors sur l'essence même du progrès qu'offre l'IA dans notre société dans la guerre du futur. Cela nous oblige à définir la place de l'éthique dans l'utilisation du recours à l'IA. Les auteurs du rapport Villani convergent vers le constat que cela « requiert une réflexion collective sur le pacte social ». À titre d'illustration, en France, la Commission nationale de l'informatique et des libertés (CNIL) a rendu un rapport sur « les places des algorithmes »[36] dans l'élaboration des politiques publiques. Il est intéressant d'y relever que l'une des options pour encadrer le développement, l'expression de l'IA est l'émergence d'une sorte de principe qui, à l'instar du principe du *privacy by design*, pourrait être qualifié d' « éthique *by design* ». Mais à très juste titre, la CNIL a souligné les difficultés d'une telle qualification « au stage du paramétrage de la machine, l'éthique *by design* viserait alors à anticiper les dilemmes au stade du développement, or le propre de l'éthique est de concurrencer des situations inédites, impliquant éventuellement des conflits de valeurs dont la solution doit être élaborée par le sujet ». Sur cette base, on pourrait considérer que l'éthique de la guerre du futur pourrait s'appuyer sur l'article 2 du *Traité de Lisbonne sur l'Union européenne* consacrant les valeurs de l'UE que sont la dignité, la liberté, la démocratie, l'égalité, l'état de droit, le droit des minorités, le pluralisme, la non-discrimination, la tolérance, la justice, la solidarité, l'égalité entre l'homme et la femme. Évaluant la nécessité de mieux encadrer les algorithmes, la CNIL souligne finalement le risque de confusion entre les expressions « éthiques des algorithmes et les algorithmes éthiques » et elle en conclut à l'urgence de développer ce que Gilles Dowek qualifie « d'éthique de la programmation ».

2.2.2 Les autres principes éthiques de l'IA au service de la guerre du futur

On en retiendra trois dans la guerre du futur.

La loyauté. En France, on peut se référer à l'étude annuelle de 2014 du Conseil d'État français, pour trouver une définition de la loyauté : « la loyauté consiste à assurer, de bonne foi, le service de classement ou de déférencement, sans chercher à altérer, le détourner, à des fins étrangères à l'intérêt des utilisateurs ». Pour la CNIL, la

36. Rapport sur les enjeux éthiques des algorithmes et de l'intelligence artificielle, CNIL, 15 décembre 2017, en ligne : <https://www.cnil.fr/fr>.

loyauté réside aussi « dans la notion d'intérêt des utilisateurs » et elle propose même une agence de notation en ce sens pour les algorithmes. La loyauté est donc bien un principe à la fois éthique et juridique qui gouverne d'ailleurs déjà les relations entre l'Union européenne et ses États membres. Les auteurs du rapport Villani ont souligné l'importance d'intégrer l'éthique dans la formation des ingénieurs et suggèrent la création d'un comité éthique des technologies numériques et de l'IA. Ce dernier rendrait des avis sur saisine initiale par les membres du gouvernement, le président de la République et les présidents des Assemblées parlementaires. On retiendra également son autosaisine. La question d'une saisine plus large des citoyens est posée. L'éthique *by design* et la loyauté sont étroitement liées au moment de la conception de l'utilisation de la technologie.

On retrouve le principe de loyauté également dans le contenu des accords conclus par l'UE avec des États tiers pour renforcer la même prise en compte du dessein commun dans le cadre des Opérations extérieures menées au nom de l'UE. On peut viser ici la déclaration du comité ministériel conjoint UE-Canada du 4 décembre 2017 qui tend au « renforcement des liens en PSDC dans la gestion des crises, la cybersécurité, les menaces hybrides, la signature et l'échange des informations classifiées »[37].

La solidarité. L'Union européenne est « unie dans la diversité ». Cette devise se traduit notamment par l'existence d'une clause de solidarité collective dans le cadre de la lutte contre les catastrophes naturelles, mais aussi dans celle du terrorisme avec, depuis le *Traité de Lisbonne*, l'existence de la clause de défense collective en cas d'agression armée (art. 42§7 *Traité de l'Union européenne*)[38] et dans une mesure moindre, dans le cadre de la constitution de la création de la coopération structurée permanente. Ce fondement de la solidarité au sein de l'Union européenne s'est largement juridicisé et permet de renforcer la solidarité internationale en constituant l'un des fils rouges des relations entre l'ONU, l'OTAN et l'UE. Les scientifiques eux-mêmes s'en sont emparés et ils conçoivent « le progrès scientifique

37. « L'UE et le Canada : un partenariat stratégique progressiste et dynamique », Déclaration commune, 1re réunion du comité ministériel conjoint UE-Canada institué en vertu de l'accord de partenariat stratégique entre l'Union européenne et ses États membres, d'une part, et le Canada, d'autre part, Bruxelles, 4 décembre 2017, en ligne : <http://www.consilium.europa.eu/media/32172/20171204-clean-joint-statement-re01fr17.pdf>.
38. Versions consolidées du Traité sur l'Union européenne et du Traité sur le fonctionnement de l'Union européenne, *Journal officiel de l'Union européenne*, no C 326 du 26/10/2012, p. 1-390.

non pas pour prôner l'espérance aveugle en la technologie, mais pour poser les jalons d'une solidarité européenne »[39].

La confiance. Elle se travaille et ne naît pas en un jour ! En revanche, le manque de confiance est évident lorsque, par exemple, la Chambre des représentants américaine vote, le 12 janvier 2018, le renouvellement du programme de surveillance d'Internet par la NSA, sans mandat, pour une durée de six ans pour recueillir des communications électroniques des suspects étrangers vivant hors des États-Unis. Le manque de confiance, c'est aussi la réaction normale face à la désinformation qui existe déjà dans la conception de la guerre du futur. Vieille comme la Première Guerre, aujourd'hui, cette désinformation envahit tous les continents. Ainsi, la France discute-t-elle actuellement une proposition de loi relative à la lutte contre les fausses informations qui renforcera considérablement les pouvoirs du Conseil supérieur de l'audiovisuel, érigé en gardien de la confiance numérique, ainsi que les sanctions par les juridictions compétentes[40]. Découle de ce principe de confiance une *obligation de vigilance* pour combattre « la toxicité présente sur l'Internet »[41]. La vigilance devient ainsi un principe méthodologique de la confiance. Elle doit accompagner les personnes sur les réseaux sociaux et traduire l'émergence d'une culture collective de la vigilance des usages sur l'Internet. Dès lors, les concepteurs d'algorithmes doivent-ils favoriser l'intelligibilité de leur conception, ce qui présuppose la transparence, notamment dans la conception des algorithmes. Mais se pose alors la question de la gestion des règles de protection de la propriété intellectuelle. La CNIL en déduit très justement que « l'intelligibilité sera la condition du déploiement du principe de loyauté »[42]. C'est en ce sens que la CNIL suggère de « prévoir que le déploiement d'un système algorithmique doit donner nécessairement lieu à l'attribution explicite des responsabilités impliquées »[43]. La question de la responsabilité doit se concevoir du concepteur à l'utilisateur final. L'orientation stratégique est clairement affirmée dans le rapport Villani qui inscrit la confiance au cœur de la dynamique forte qui accompagne l'IA en sécurité et en défense[44]. Les outils préconisés mis au service de cette confiance s'appuient sur

39. Jean-Gabriel GANASCIA cité par Charles THIBOUT, « L'Europe peut-elle faire face à la révolution scientifique en cours ? », *Institut des relations internationales et stratégiques*, en ligne : <http://www.iris-france.org>.
40. Proposition n° 799 de loi relative à la lutte contre les fausses informations du 21 mars 2018 présentée notamment par Richard FERRAND, site de l'Assemblée nationale.
41. Richard KHOURY, *Progrès et enjeux de l'intelligence artificielle*, UNIDEF 9, *La guerre du futur*, Université Laval, 1er mars 2018.
42. Rapport de la CNIL, *supra*, note 36.
43. *Ibid*.
44. Voir Cédric VILLANI, *supra*, note 8.

le recours aux marchés publics concernant l'imagerie (satellitaire, drones et l'hyper spectral), la vidéo, les signaux électromagnétiques (radars, systèmes de combats, le renseignement, la cybersécurité, la robotique notamment) et les données de maintenance. Dans tous ces secteurs sensibles, un cadre régalien d'action fort est préconisé pour préserver les intérêts essentiels de l'État, mais il devra trouver un équilibre avec le respect des droits fondamentaux[45]. On retrouve cette même démarche de la recherche de la confiance par l'expression « une préférence patriotique » française, qui n'est pas si éloignée de celle canadienne qui vise à « protéger les renseignements personnels des Canadiens à la frontière des USA »[46]. Ce foisonnement de prises de positions politiques montre combien le sujet est sensible, témoignant souvent d'un déficit de confiance de la part des peuples qu'ils représentent. Et pourtant, l'IA doit être acceptée comme une source de progrès dans la guerre du futur. La substitution de la personne par le robot n'évite certes pas les troubles *post*-traumatiques, mais protège la vie du soldat. L'IA sera donc effectivement « un fort appui en matière de simulation opérationnelle et permet une amélioration dans la performance et l'augmentation des systèmes de combat dans le cadre de la logistique et de la maintenance »[47]. L'IA est caractérisée par le changement de vitesse qu'elle impose à notre société, comme l'est souvent le progrès scientifique. Cette modernité technologique doit, dans le cadre de services régaliens, épouser l'effectivité de la protection des intérêts essentiels de l'État et devra être au service de la protection du secret. Elle nous oblige déjà à repenser notre approche du « besoin de connaître » l'information pour rester au service d'un État protecteur[48], mais aussi d'un État offensif dans le cyberespace grâce, en France, au Comcyber[49].

45. Cédric VILLANI, *supra*, note 8.
46. Rapport présenté à la Chambre des communes de M. Bob Zimmer, président du comité permanent de l'accès à l'information de la protection, des renseignements et de l'éthique, décembre 2017.
47. Cédric VILLANI, *supra*, note 8.
48. Rapport sur le secret de la défense nationale, Secrétariat Général de la Sécurité et de la Défense nationale, 30 janvier 2018.
49. *La cyberdéfense à l'horizon 2025*, promotion Louise de Bettignies du Master 2 Sécurité Défense et Intelligence Stratégique, SEDEFIS, rapport de prospective réalisé sous la direction du général Philippe Boone, Sciences Po Rennes, mai 2018.