MORTELS ALGORITHMES

Du code pénal au code létal

Par Susan Schuppli
Traduit de l'anglais par Lucie Gerber
Paru dans la revue Radical Philosophy, 187 (sept/oct 2014)

La guerre des drones menée par le gouvernement Obama, et coordonnée par John Brennan, responsable de la Homeland Security, tend à automatiser le règlement des conflits dans lesquels sont engagés les États-Unis (en Afghanistan, Pakistan, Somalie et Yemen notamment). Dans ce nouveau mode opératoire, les machines ne se contentent plus d'exécuter les mises à mort, elles les décident. Cette robotisation de la hiérarchie militaire pose des questions juridiques, encore sans réponse, et lourdes d'implications éthiques. Si des algorithmes ont à la fois la capacité d'établir qui doit être tué et d'exécuter cette décision via des robots, qui peut être tenu responsable du meurtre ?

Susan Schuppli est vice-directrice du Centre de recherches en architecture à l'université Goldsmith de Londres. Avec Eyal Weizman, architecte analysant, entre autres, les formes du conflit israélo-palestinien, elle participe au projet « Forensic Architecture », travaillant sur les manifestations urbaines, architecturales et spatiales de la violence, et sur les représentations de l'espace (cartes, images satellites, images 3D) qui accompagnent et structurent les débats portant sur le conflit, principalement armés.

Cela fait déjà longtemps que des algorithmes se sont mis à prendre toutes sortes de décisions concernant les activités vitales sur lesquelles reposent notre bien-être et notre survie : depuis les *pacemakers* qui assurent le maintien des rythmes cardiaques naturels, jusqu'aux algorithmes génétiques [i] qui optimisent les temps de réaction en croisant données d'emplacement des ambulances et données démographiques, en passant par les systèmes d'alerte rapide qui suivent au plus près l'approche des tempêtes, détectent l'activité sismique et s'évertuent même à prévenir les génocides en surveillant, via des images prises par satellites, des zones menacées par des conflits ethniques[1]. Mais les algorithmes se sont aussi vus confier d'autres tâches. Parmi elles, la mise à mort. Les lignes de code exécutées servent alors, à leur tour, littéralement, à exécuter.

La présidence Obama est persuadée que la guerre contre le terrorisme peut être gagnée grâce à l'utilisation de logiciels prédictifs qui permettraient de surpasser informatiquement (*out-computing*) ses ennemis, et de contrecarrer ainsi les menaces terroristes. Guidée par cette conviction, une nouvelle génération d'algorithmes meurtriers est en train d'être conçue, qui vont à la fois contrôler et gérer la « *kill list* [ii] », et,

i. Les algorithmes génétiques opèrent analogiquement sur les principes de l'évolution des espèces (enjambements, mutations et sélection), NdT.

ii. Base de données listant les informations au sujet des ennemis à abattre sans procès public ni conventionnel, utilisée par le gouvernement Obama au sein de la « Disposition Matrix » (sic), et mise en application principalement par des attaques de drones. John Brennan, en charge du département Homeland Security est le principal coordinateur de cette *kill list*, faisant dire au *New York Times*, qu'il est « *probablement l'homme qui a eu le plus de pouvoir et d'influence dans une position comparable au cours des 20 dernières années* ». Robert Mazzetti, Mark Shane Scott, « Drone Strikes' Dangers to Get Rare Moment in Public Eye ». *The New York Times*, 5 fév. 2013.

en conséquence, décider des frappes[2]. La pratique (récemment abolie) des « frappes de signatures », dans lesquelles l'analyse de données établissait des comportements « terroristes » typiques et associait ces « schémas (*patterns*) » à des cibles potentielles sur le terrain, permet d'entrevoir un avenir où la collecte de renseignements, leur évaluation et l'intervention militaire, y compris les calculs déterminant qui peut être tué en toute légalité, seront essentiellement réalisés par des machines, à partir d'une base de données agrégeant un nombre croissant d'informations. Contrairement à ce qui a été maintes fois suggéré, cette transition vers un mode d'exécution régi par des algorithmes n'est donc pas une simple continuation de la mise à mort à distance, prolongeant l'invention de l'arc et de la flèche qui instaurèrent une distance spatiale entre le guerrier et son ennemi[3]. Cette transition est aussi la conséquence d'une automatisation croissante de la guerre, héritière du couplage cybernétique de la théorie mathématique de l'information de Claude Shannon et des recherches liées à l'effort de guerre de Norbert Wiener sur les boucles de rétroaction et les systèmes de contrôle de la communication[4]. À l'ère des systèmes d'armement intelligents, le contrôle des opérations militaires et la prise de décision sont de plus en plus sous-traités à des machines.

Terreur informatique

En 2011, le département de la Défense américain (Department of Defense, DoD) rendait publique sa « feuille de route » prévoyant d'accroître le recours aux technologies *sans équipage* [*unmanned*, c'est-à-dire « sans humain »]. Parmi celles-ci, les systèmes aériens sans pilote – les drones – ne sont qu'un aspect d'une stratégie globale visant l'implémentation d'agents intelligents totalement autonomes. Voici comment le DoD envisage son propre futur :

Le DoD a le projet d'intégrer les différentes ressources d'équipements sans équipage. Elles dotent le programme Joint Warfighters de solutions flexibles et permettent en même temps d'exploiter les avantages inhérents aux technologies sans équipage, tels que la persistance, la taille, la rapidité, les facilités de manœuvre et le risque réduit pour la vie humaine. Tandis que les systèmes sans équipage opéreront en continuité avec les systèmes avec équipage [*manned*], le DoD prévoit de réduire progressivement le degré d'emprise humaine sur le contrôle et la prise de décision nécessaires pour opérer la partie sans équipage des forces armées[5].

Le document du DoD est un curieux mélange de caricature de la guerre froide et de fordisme, sur fond d'inquiétudes géopolitiques contemporaines. On y trouve deux petites scènes fictionnelles qui illustrent la manière dont les systèmes autonomes pourraient améliorer l'efficacité des opérations en favorisant l'interopérabilité des domaines militaires. L'objectif est d'accroître les moyens d'intervention de l'armée américaine, de l'Air Force et de la Navy, en jouant sur la complémentarité entre les portions sans et avec équipage de leurs forces armées. Il est frappant de constater à quel point l'intrigue et le *casting* de ces scénarios d'anticipation sont familiers : ils mettent en scène l'approvisionnement national en ressources hydrocarbures menacé par des acteurs voyous équipés de technologies russes. Dans l'un de ces scénarios, un État-nation islamique radicalisé s'est doté d'un vieux sous-marin nucléaire russe qui, surpris par un tremblement de terre dans le Pacifique, contamine les eaux littorales de l'Alaska et menace ses réserves de pétrole. L'autre scénario nous transporte dans le Golfe de Guinée au large des côtes africaines, et concerne le sabotage d'un oléoduc sous-marin, aggravé par l'approche d'un vaisseau hostile capable de lancer un missile russe air-sol de courte portée[6].

Ces saynètes, qui empruntent aux films d'action hollywoodiens, sont longuement développées dans cinq pleines pages du rapport. Elles tranchent avec les exigences de sérieux scientifique, de prudence politique et de rationalisation économique qui, le document l'assure à maintes reprises, guident la transition vers les systèmes totalement dépourvus d'équipage [iii]. À quel titre devraient nous convaincre ces projets et ces stratégies ? Au nom d'un imaginaire culturel collectif qui puise sa politique dans les laboratoires d'imagerie de synthèse de l'industrie de l'info-divertissement ? Ou bien, faut-il plutôt en appeler à une approche fondée sur les preuves, que l'on appliquerait à la résolution des problèmes complexes posés par l'évolution des contextes globaux ? Sans surprise, le rapport est extrêmement détaillé (et techno-fétichiste) dans sa description des réponses robotisées à ces scénarios de situations à risque. Il l'est en revanche beaucoup moins dans son traitement des trois principaux défis identifiés comme spécifiques au recours croissant aux systèmes automatisés et autonomes :

1. L'investissement dans la « Science et technologie (S&T) » pour augmenter l'opérationnalité des systèmes autonomes.
2. Le développement de règles et de recommandations pour définir le type de décision qui peut être délégué de manière sûre et éthique à des machines et pour spécifier les conditions de cette délégation.
3. Le développement de nouvelles techniques de « Vérification et validation (V&V) » et de « Test et évaluation (T&E) » pour réaliser les conditions d'une « confiance » vérifiable dans l'autonomie[7].

Le second de ces défis (la délégation de la prise de décision aux systèmes informatiques) soulève un point crucial. Il engendre de profonds dilemmes éthiques et met en cause la capacité des cadres juridiques existants à prendre en

iii. Sur l'influence des scénarios de films hollywoodiens dans les rapports officiels de la Défense états-unienne, notamment autour du paradigme « Terminator », voir « Et vous trouvez ça drone ? Enquête sur l'automatisation de la guerre et la robotisation de la police », *Revue Z n°2*, Automne 2009.

iv. La *common law* vise le droit des pays issus de la tradition juridique britannique. Les systèmes juridiques de *common law* reposent sur la règle du précédent selon laquelle le juge doit respecter les règles posées par ses pairs dans des décisions antérieures. Le droit de la *common law* se construit donc à partir des décisions prises par les juges dans des cas concrets, par opposition aux systèmes dits de droit continental, comme la France, où le droit est issu de règles posées par le législateur et compilé dans des codes. Cette opposition est bien évidemment schématique, dès lors que la jurisprudence joue un rôle important en France, de même que les États-Unis disposent d'un corpus législatif qui s'impose aux juges, NdT.

compte l'émergence de ces nouveaux acteurs algorithmiques. La question est d'autant plus épineuse que la logique jurisprudentielle qui organise la prise de décision juridique (dans la tradition de la *common law* [iv]) suit le même cheminement que celui qui a organisé le programme drone dès son origine : à savoir la justification d'une action par l'existence d'un modèle [*pattern*] comportemental, établi à partir d'événements antérieurs.

L'aporie juridique recoupe un discours parallèle sur la responsabilité morale. Ce débat, beaucoup plus général, a eu tendance à présenter le recours aux drones armés en termes d'antagonisme humains-machine. Comme l'ont écrit les auteurs de l'entrée « Informatique et responsabilité morale » de la *Stanford Encyclopedia of Philosophy* :

Les débats philosophiques sur la responsabilité ont traditionnellement pris pour cible les composantes humaines de l'action morale. Lorsqu'il s'agit d'assigner une responsabilité morale, on présuppose ordinairement des agents humains qui accomplissent des actions aux conséquences immédiates et bien définies. Dans une société où la technologie occupe une place toujours plus importante, l'activité humaine ne peut être correctement comprise sans se référer aux artéfacts technologiques, ce qui n'est pas sans compliquer l'assignation d'une responsabilité morale[8].

Lorsqu'on interroge les conditions qui rendraient moralement acceptable de tuer délibérément un être humain, il n'est pas spécifiquement question de savoir si le droit autorise pareil acte, pour des raisons de menace imminente, de légitime défense, voire même d'empathie pour une personne souffrant d'une douleur extrême ou dans un état végétatif permanent. Le registre moral dans lequel s'élabore la décision de tuer relève d'un cadre éthique différent : un registre selon lequel l'individu n'est pas nécessairement lié à un contrat conclu entre le citoyen et l'État. Tandis que les positions morales peuvent être propres à des valeurs ou à des croyances individuelles, les cadres juridiques nous permettent d'agir en notre nom collectif, en tant que citoyens liés contractuellement à un corps représentatif, démocratiquement élu, agissant en notre nom, bien que nous puissions être en désaccord politique avec lui.

Il est donc beaucoup plus simple de prendre moralement position contre des événements – les frappes de drones américains au Pakistan –que de prouver leur illégalité, compte tenu de la législation anti-terroriste qui a été mise en place depuis le 11 septembre 2001. Il devient encore plus difficile d'assigner une responsabilité morale, de prouver une faute pénale de négligence ou de démontrer une responsabilité juridique pour un événement meurtrier lorsque humains et machines interagissent pour prendre des décisions. Cette complexification ne pourra que s'accroître avec le perfectionnement des systèmes automatisés, qui agiront de plus en plus comme des agents légaux indépendants. De plus, depuis l'arrêt Daubert, rendu en 1993 par la Cour suprême des États-Unis dans le cadre d'un procès intenté contre l'entreprise Merrel Dow Pharmaceuticals, il revient à la sphère judiciaire de déterminer l'admissibilité d'une preuve scientifique [v]. Il est donc devenu difficile pour les instances judiciaires d'adopter une position militante, dans la mesure où elles sont confrontées à leurs propres limites dans la compréhension des innovations techniques. Aujourd'hui, il serait manifestement déraisonnable de traduire un algorithme devant les tribunaux si les choses tournaient mal sur le terrain, encore moins lorsque les opérations sont parfaitement exécutées, comme dans le cas d'une frappe létale de drone.

En me focalisant sur les dimensions légales de la responsabilité algorithmique plutôt que sur des questionnements moraux plus généraux, je n'entends pas suggérer que la morale et le droit doivent être reléguées à des sphères séparées. Il est toutefois utile d'engager une première réflexion sur les effets des algorithmes, car ils ne se contentent pas de réordonner les principes qui régissent nos vies, mais peuvent aussi fournir de nouveaux agencements éthiques dérivés d'axiomes mathématiques.

Responsabilité algorithmique

Le droit a déjà étendu la catégorie de « personnalité juridique » de sorte à y inclure des acteurs non-humains tels que les entreprises (qualifiées de « personnes morales »). Cette notion permet de réfléchir à la question de la responsabilité algorithmique[9]. On peut bien sûr faire valoir que les méthodes juridiques ne constituent pas le meilleur cadre pour résoudre des dilemmes moraux. Mais il faut ajouter que rien n'indique par ailleurs que les objectifs du contre-terrorisme soient mieux remplis au moyen d'une supervision algorithmique. De toute façon, mettre l'accent sur la prise en compte du raisonnement algorithmique par le droit peut s'avérer utile dans une situation où nous sommes confrontés à la possibilité bien réelle que la « *kill list* », ou d'autres matrices émergentes pour la conduite de la « guerre contre le terrorisme », se fondent sur des algorithmes, relevant d'assemblages socio-techniques plus vastes, à l'intérieur desquels il devient impossible de dissocier agents humains et non-humains. Nos exigences face au droit ne peuvent que s'en trouver plus élevées.

Face à ces rapides développements technologiques, on peut légitimement s'inquiéter du degré de réactivité des règles de droit, de leur capacité à soumettre les systèmes algorithmiques aux mécanismes régulateurs qui s'imposent habituellement aux forces qui affectent la société dans son ensemble[10]. Toutefois, le terrain a déjà été préparé pour l'émergence d'une nouvelle catégorie d'acteurs juridiques : les systèmes intelligents. S'ils ne disposent pas à proprement parler d'un libre arbitre au sens classique du terme (qui permettrait de leur assigner une responsabilité pénale), ils ont néanmoins été dotés d'une forme d'auto-détermination. Ils ont en effet été programmés pour prendre des décisions en se fondant sur leur propre logique algorithmique[11]. Les drones de combat ne sont que la partie émergée de l'iceberg des systèmes militaires automatisés mis en service par le DoD. Ils ne sont qu'un élément dans un ensemble plus vaste de dispositifs télé-pilotés qui agiront à partir des données qu'ils auront eux-mêmes collectées, gérées et analysées.

v. Par l'arrêt Daubert, les juges de la Cour suprême des États-Unis ont fixé des règles permettant de déterminer si le témoignage scientifique d'un expert peut être recevable en justice, NdT.

Ceux qui prônent la délégation de la prise de décision aux algorithmes ne tarissent pas d'éloges sur la quasi-instantanéité des réactions qui permettent aux agents intelligents – qualifiés par certains de « prédateurs moraux » – de faire des ajustements, à la milliseconde près, pour éviter une frappe de drone si, par exemple, des enfants venaient à sortir d'une maison prise pour cible comme un repaire de miliciens [12]. L'idée, qui n'est pas neuve, est que les systèmes robotiques peuvent réduire la marge d'erreur et compresser les pertes civiles qui sont souvent la conséquence des actions menées sur le terrain par des soldats fatigués. Les machines ont également cet avantage qu'elles ne se soucient pas outre mesure de leur propre conservation. Par contraste, les soldats se préoccupent de leur survie et peuvent, sous l'effet de la fatigue par exemple, commettre des erreurs de jugements. Mais, demandent les juristes Sabine Gless et Herbert Zech, si ces « agents intelligents sont souvent utilisés dans des zones où les risques d'échec et d'erreur peuvent être réduits en substituant des machines aux humains, la question se pose : qui est responsable si les choses tournent mal[13] ? »

Lorsqu'un acte a entraîné des préjudices corporels ou des accidents mortels, le débat juridique a généralement pour objet l'évaluation du degré de prévisibilité de telles conséquences. Pour se prononcer sur le cas porté à leur attention, la question est de savoir si tous les efforts raisonnablement envisageables et tous les protocoles préventifs possibles ont été intégrés au système pour réduire la probabilité d'occurrence de ce type de conséquence. Toutefois, lorsque les programmateurs fixent les conditions dans lesquelles une machine sera amenée à prendre une décision, ils ne peuvent évidemment pas intégrer toutes les variables potentiellement en jeu. Le problème est d'autant plus épineux que les conditions au sol et la connaissance des événements qui s'y déroulent sont aussi variables que les contextes changeants de conflits et du contre-terrorisme. Werner Dahm, directeur scientifique de l'United States Air Force, souligne la difficulté qu'il y a à concevoir des systèmes « zéro erreur » : « Vous devez être capable de montrer que le système ne va pas mal tourner – il vous faut donc invalider une hypothèse négative[14]. »

Dans la mesure où les processus de prise de décision fortement automatisés impliquent des contextes complexes en évolution rapide, saisis au prisme de technologies multiples, pouvons-nous raisonnablement espérer intégrer une forme quelconque de décision éthique dans ces systèmes sans équipage ? Une approche algorithmique des problèmes éthiques soulevés par la guerre des drones reproduira-t-elle la logique qui présidait aux frappes de signature, je veux parler d'une forme de raisonnement consistant à établir des suspicions à partir d'un schéma comportemental ou d'une activité militante ? Faut-il, par exemple, tuer Abdulrahman al-Awlaki, un jeune homme âgé de 16 ans vivant au Yemen, parce que son père était un religieux radicalisé ; un rôle qu'il est susceptible d'hériter[15] ? La « *kill list* », que l'on connaît depuis peu sous la formule euphémique de « Disposition Matrix », suggère que les modèles informatiques peuvent servir à prendre ce type de décision. Comme le souligne le journaliste du *Washington Post* Greg Miller : « La matrice contient les noms des personnes soupçonnées de terrorisme. Elle répertorie pour chacun d'entre eux l'ensemble des ressources qui sont mobilisées pour les traquer, y compris les actes d'accusation scellés et les opérations secrètes[16]. »

Si l'on peut considérer les systèmes intelligents comme des agents légaux, ils n'ont pas encore été dotés d'une personnalité juridique. Des précédents existent cependant qui portent en germe cette possibilité. L'idée selon laquelle, derrière chaque machine, il y aurait un être humain ou une « personnalité juridique » – un agent auquel on pourrait en fin de compte assigner une responsabilité, pour le meilleur ou pour le pire – n'est plus tenable. Cette conception omet que les systèmes complexes sont rarement, voire jamais, le produit d'un auteur unique, et que les humains et les machines n'opèrent pas dans des sphères séparées. En effet, ils sont si intimement liés que la notion même d'agent humain souverain, exempt de toute médiation par la machine semble tout à fait improbable.

Que l'on considère un instant un aspect seulement de la guerre des drones au Pakistan : celui de la logistique aérienne des États-Unis. Le simple fait de maintenir un drone Predator dans les airs pendant 24 heures, soit la moitié de la durée d'une mission ordinaire, mobilise plus de 165 personnes. Ces besoins en personnel sont eux-mêmes intégrés dans des systèmes socio-techniques multiples, composés de sous-traitants militaires, d'officiers du renseignement, de spécialistes de l'analyse de données, de juristes, d'ingénieurs, de programmateurs, mais aussi de matériel, de logiciels, de communications par satellites et de centres d'opération (Combined Air Operations Centre, CAOC), etc. Sans compter l'infrastructure de Recherche et développement (R&D) qui conçoit les systèmes sans équipag , élabore les procédures pour les rendre opératoires et procèdent aux tests préliminaires, ni l'appareil administratif qui a réuni tous ces acteurs pour créer l'événement que l'on appelle une « Frappe de drone »[17].

Dans le cas d'un système complètement automatisé, la prise de décision dépend de boucles de rétroaction [*feedback*] qui injectent constamment de nouvelles informations dans le système et le recalibrent. De façon plus significative encore en termes de responsabilité juridique, la prise de décision dépend aussi de la capacité du système à s'auto-éduquer : la possibilité pour les algorithmes d'apprendre et de modifier les séquences qui les codent, indépendamment de toute supervision humaine. Chercher, comme l'exige aujourd'hui le droit pénal, à isoler l'agent singulier directement (c'est-à-dire légalement) responsable d'un accident mortel, conduit à penser que seul le bureau exécutif du président des États-Unis pourrait, en fin de compte, être tenu responsable des conditions composites qui, enchaînées les unes aux autres, aboutissent à une frappe de drone, et avec elle, à l'éventualité de victimes civiles.

Étant donné que les États-Unis ne reconnaissent pas la compétence de la Cour pénale internationale et l'article 25 du statut de Rome fixant les règles en matière de responsabilité pénale individuelle, quelles seraient dès lors les formules juridiques nouvelles qui pourraient être créées pour rendre compte d'une causalité indirecte et composite, laquelle recouvre toute une série de règles relatives à la réparation des préjudices résultant de fautes civiles, pourrait servir de modèle, utile dans ces questionnements.

Les procédures judiciaires relatives à l'émission de produits polluants dans l'environnement sont à ce sujet particulièrement instructives. La pollution atmosphérique est un phénomène très répandu et ses effets létaux ne se manifestent souvent qu'après plusieurs décennies, impliquant un ensemble également complexe d'agents humains et non-humains. Les actions en justice dans des cas de pollution atmosphérique se sont frayées un chemin devant les tribunaux, bien que l'issue en ait généralement été défavorable pour les plaignants. Dans ce domaine, les contentieux les plus marquants résultent d'actions de groupe, menées par de nombreux plaignants en matière de préjudice lié à des produits toxiques, et notamment le recours à l'agent orange comme défoliant au Vietnam ou la catastrophe du Bhopal en Inde[18]. Mais en dernier ressort, l'efficacité de cette approche doit être jugée à la lumière du résultat escompté par l'assignation d'une responsabilité : dans les cas que je viens de mentionner, la démarche visait moins la dissuasion ou la punition que des dommages et intérêts réparant les préjudices subis.

Reprogrammer la loi

Les machines peuvent être conçues de manière à incorporer un degré supérieur d'intentionnalité, et leurs performances dépasseront, dans bien des cas, celles des humains. Le développement des systèmes sans équipage devra dès lors prendre en compte un nombre plus grand de variables pour déterminer si les conditions d'une exécution sont remplies, y compris les contextes géopolitiques changeants et les cadres juridiques incertains. La mise au point de mécanismes de sûreté intégrés contribuent à créer les conditions d'un régime de prise de décision proto-morale, interrompant une intervention lorsque surgissent dans le champ d'action des sujets humains d'une taille spécifique (des enfants), d'un âge ou d'un sexe déterminés (des mâles de moins de 18 ans). Mais, politiquement parlant, faut-il vraiment se focaliser sur l'intégration de contraintes éthiques au développement des systèmes télé-pilotés lorsqu'on veut contrecarrer le scénario d'une mise à mort par algorithmes ? Dit autrement, nous est-il encore possible de saper l'impunité dont jouissent actuellement certains assemblages socio-techniques ? Comme l'affirme en 2009 un rapport de la Royal Academy of Engineering consacré aux systèmes autonomes :

La gouvernance des systèmes autonomes peut difficilement se fonder sur les modèles juridiques et réglementaires qui se réfèrent aux systèmes gérés par des opérateurs humains. De plus, dans sa forme présente, le droit établit une distinction entre opérateurs humains et systèmes techniques et exige qu'un agent humain soit responsable d'un système autonome et automatisé. Toutefois, les technologies qui sont utilisées soit pour augmenter les performances humaines soit pour compenser des déficits cognitifs ou moteurs sont susceptibles de générer des agents hybrides… En l'absence d'un cadre juridique pour les technologies autonomes, il existe un risque que ces agents essentiellement humains ne puissent être jugés légalement responsables de leurs actions – reste alors à savoir qui pourrait encore l'être[19].

Une stratégie juridique plus efficace pourrait être d'impliquer un ensemble plus large d'agents, y compris algorithmiques, qui apportent leur concours à la réalisation d'actes de ce type, même si l'élargissement des limites de la responsabilité pénale est un processus complexe. Comme le formule l'« Étude sur la responsabilité pénale au Sri Lanka », publiée en 2009 par l'European Center for Constitutional and Human Rights : « Les individus qui exercent le pouvoir de rendre possible les crimes qui ont été commis, peuvent être tenus pénalement responsables comme auteurs du crime. C'est au sein des ministères civils, tels que le ministère de la Défense ou le Bureau du président, que l'on trouve habituellement les auteurs de ces crimes[20]. » Descendre le long de la hiérarchie et se focaliser sur ceux qui participent à la production de violence en exécutant des ordres a été une stratégie juridique payante dans certains cas (Sri Lanka). Mais elle s'est aussi révélée problématique dans les cas (Abu Ghraib) où l'inculpation d'officiers de rang subalterne a rompu la chaîne de relations causales qui pouvait impliquer des acteurs plus haut placés. Bien entendu, si l'objectif est la sanction, il n'y a aucun sens à traduire un algorithme devant la justice pour avoir exécuté des ordres aux conséquences mortelles, le système ayant justement été conçu pour les réaliser. Dès lors, la démarche doit s'inscrire dans une stratégie globale visant à étendre le champ de la causalité, en vue d'élargir la portée de la responsabilité juridique.

Mon propre travail de recherche au sein du Forensic Architecture projet, aux côtés d'Eyal Weizman et de beaucoup d'autres, consiste à développer de nouvelles méthodes d'investigation spatiale et visuelle pour appuyer le travail d'enquête des Nations Unies sur l'utilisation des drones armés. Ce travail offre un point de vue spécifique pour réfléchir à la manière dont les « champs machiniques » sont en train de recomposer ceux de l'action politique, appelant à concevoir de nouvelles stratégies juridiques[21]. Si l'on prend au sérieux la capacité d'action dont les « choses » disposent, nous devons aussi considérer la capacité à agir de celles dont le champ de production est mis au service de la décision même de tuer. En opérant largement au-delà des limites de la perception humaine, les calculs par ordinateur ont produit des conjonctions informatiques qui ont redistribué et transformé les espaces au sein desquels se produit l'action. La nature même de ces actions lourdes de conséquences a été modifiée. Lorsqu'on enrôle des algorithmes pour l'emporter contre le terrorisme et pour calculer qui peut et doit être tué, n'est-il pas nécessaire de produire une politique adaptée à ces formes très radicales de calcul, ainsi qu'un cadre juridique suffisamment souple pour délibérer sur des événements de ce type ?

Confier la prise de décision à des systèmes automatisés produira de nouveaux rapports de pouvoir pour lesquels nous ne disposons pas encore de cadres juridiques ou de modes de résistance politique adaptés. Il est peut-être plus important encore de noter que nous n'avons pas de compréhension collective suffisante de la manière dont ces décisions peuvent être prises et fondées. Comme le suggère l'arrêt *Daubert*, le savoir scientifique sur les processus techniques n'appartient pas exclusivement au domaine de la science. Les exigences de responsabilité et de supervision publiques nécessiteront toutefois un degré de participation plus grand dans les cadres épistémologiques qui organisent et contrôlent ces systèmes socio-techniques. Le défi sera vraisemblablement, pour nous tous, considérable. Quel type d'assemblée publique serait à même de contrecarrer la clôture prématurée de ce que Bruno

Latour appelle une certaine « épistémologie des faits », aujourd'hui dissimulés sous un voile de secret appelé « la sécurité nationale » – ce même état de faits qui dessine la feuille de route du DoD pour les systèmes de drone ?

Dans une récente interview donnée à la chaîne de radio ABC, Sarah Knuckey, directrice du « Project on Extrajudicial Executions » de la New York University Law School, soulignait que la guerre des drones a rudement éprouvé les conventions internationales et, dans le même élan, la protection des civils[22]. Les « règles de la guerre » sont « déjà désespérément désuètes », affirme-t-elle, et vont exiger « l'élaboration de nouvelle obligations » : « Je constate un fort degré d'inquiétude au sujet des pratiques actuelles des États-Unis et des règles qui les sous-tendent. Mais, dans une perspective de long terme, en particulier du point de vue des avocats qui exercent en dehors des États-Unis, il y a lieu de s'inquiéter non seulement de ce qu'il se passe aujourd'hui, mais aussi de ce que cela signifiera dans dix, quinze ou vingt ans.[23] »

Ces nouvelles obligations – ces nouvelles règles juridiques – pourront-elles jouer un rôle préventif similaire à celui des logiciels et des technologies qui sont en cours de développement, ce que j'appellerai un *sens projectif* du droit ? Pourraient-elles s'inspirer de l'esprit des Conventions de Genève qui protègent les droits des non-combattants, plutôt que des protocoles, qui à l'instar des Conventions de la Hague de 1899 et de 1907, définissent l'usage des armes de guerre. Ces conventions, sont en effet réactives dans leur formulation et centrées sur des événements. Si tel était le cas, si nous choisissions de nous inspirer de ces Conventions, il faudrait considérer un cadre juridique qui ne soit pas tant réglé par une logique jurisprudentielle – par ce qui est advenu dans le passé – mais, plutôt, par ce qui pourrait arriver dans le futur.

À lire également :

« Géographie du drone », Derek Grégory, traduction par Émilien Bernard, *Jef Klak n°1 (Marabout)*, en librairie.

« Israël et la "guerre humanitaire" », Eyal Weizman, traduction par Rémy Toulouse, *Article 11*.

Théorie du drone, Grégoire Chamayou, éd. La Fabrique, en librairie.

La vie algorithmique, Critique de la raison numérique, Éric Sadin, éd. L'échapée, en librairie.

NOTES

1. Voir, par exemple, le recours aux images satellite dans des programmes de surveillance et de documentation des exactions : « Eyes on Darfur » (www.eyesondarfur.org) et « The Sentinel Project for Genocide Prevention ».

2. Cori Crider, « Killing in the Name of Algorithms : How Big Data Enables the Obama Administration's Drone War », *Al Jazeera America*, 2014, consulté le 18 mai 2014. Voir aussi l'organigramme dans Daniel Byman et Benjamin Wittes, « How Obama Decides Your Fate if He Thinks You're a Terrorist », *The Atlantic*, 3 janvier 2013.

3. Pour une analyse récente des géographies multiples et composites dans lesquelles sont menées les opérations de drones, voir Derek Gregory, « Drone Geographies », *Radical Philosophy* 183 (janvier/février 2014), pp. 7–19.

4. Les théoriciens de l'information contemporains affirmeraient que le modèle des boucles de régulation et de rétroaction de la cybernétique du second ordre ne prend pas en considération le caractère imprévisible des données évolutives internes au système, qui résulte du traitement de bases de données en expansion. Voir l'introduction de Luciana Parisi à *Contagious Architecture : Computation, Aesthetics, and Space*, MIT Press, Cambridge MA, 2013. Pour une discussion de la cybernétique de Wiener dans ce contexte, voir Reinhold Martin, « The Organizational Complex : Cybernetics, Space, Discourse », *Assemblage* 37, 1998, p. 110.

5. DOD, *Unmanned Systems Integrated Roadmap Fy2011–2036*, Office of the Undersecretary of Defense for Acquisition, Technology, & Logistics, Washington, DC, 2011, p. 3, lien.

6. *Ibid.*, pp. 1–10.

7. *Ibid.*, p. 27.

8. Merel Noorman et Edward N. Zalta, « Computing and Moral Responsibility », *The Stanford Encyclopedia of Philosophy* (2014).

9. Voir John Dewey, « The Historic Background of Corporate Legal Personality », *Yale Law Journal*, vol. 35, no. 6, 1926, pp. 656, 669.

10. Data & Society Research Institute, « Workshop Primer : Algorithmic Accountability », *The Social, Cultural & Ethical Dimensions of 'Big Data'* workshop, 2014, p. 3.

11. Voir Gunther Teubner, « Rights of Non-Humans ? Electronic Agents and Animals as New Actors in Politics and Law », *Journal of Law & Society*, vol. 33, no.4, 2006, pp. 497–521.

12. Voir Bradley Jay Strawser, « Moral Predators : The Duty to Employ Uninhabited Aerial Vehicles », *Journal of Military Ethics*, vol. 9, no. 4, 2010, pp. 342–68.

13. Sabine Gless and Herbert Zech, « Intelligent Agents : International Perspectives on New Challenges for Traditional Concepts of Criminal, Civil Law and Data Protection », texte pour Intelligent Agents workshop, 7–8 février 2014, University of Basel, Faculty of Law.

14. Agence-France Presse, « The Next Wave in U.S. Robotic War : Drones on Their Own », *Defense News*, 28 septembre 2012, p. 2.

15. Interrogé sur la frappe de drone qui a tué en 2011 au Yémen Abdulrahman al-Awlaki, un adolescent de seize ans né sur le sol américain et fils de Anwar Al-Awlaki, un religieux radicalisé, Robert Gibbs, l'ancien attaché de presse de la Maison Blanche et conseiller principal pour la campagne de réélection du Président Obama, répondit que le jeune homme aurait dû avoir un « père plus responsable ».

16. Greg Miller, « Plan for Hunting Terrorists Signals U.S. Intends to Keep Adding Names to Kill Lists », *Washington Post*, 23 otcobre 2012.

17. « Cela peut sembler paradoxal, mails il faut beaucoup plus de personnes pour opérer un avion sans pilote que pour faire voler les avions de guerre traditionnels. Selon l'Air Force, il ne faut pas moins de 168 personnes pour faire voler un Prédateur pendant seulement vingt-quatre heures ! Pour le drone de surveillance plus large Global Hawk, ce nombre grimpe à 300 personnes. Par contraste, il faut moins de cent personnes par mission pour un avion de combat F-16. » Medea Benjamin, *Drone Warfare : Killing by Remote Control*, Verso, London and New York, 2013, p. 21.

18. Voir Peter H. Schuck, *Agent Orange on Trial : Mass Toxic Disasters in the Courts*, Belknap Press of Harvard University Press, Cambridge MA, 1987. See also : www.bhopal.com/bhopal-litigation.

19. Royal Academy of Engineering, *Autonomous Systems : Social, Legal and Ethical Issues*, RAE, London, 2009, p. 3, lien.

20. European Center for Constitutional and Human Rights, *Study on Criminal Accountability in Sri Lanka as of January 2009*, ECCHR, Berlin, 2010, p. 88.

21. Ont fait partie de l'équipe de recherche sur les frappes de drones du projet Forensic Architecture : Jacob Burns, Steffen Kraemer, Francesco Sebregondi et SITU Research. See www.forensic-architecture.org/case/drone-strikes.

22. Bureau of Investigative Journalism, « Get the Data : Drone Wars ».

23. Annabelle Quince, « Future of Drone Strikes Could See Execution by Algorithm », *Rear Vision*, ABC Radio, edited transcript, pp. 2–3.