LAMY
REVUE

REVUE LAMY

Droit des Affaires

Dossier : le droit pénal des affaires de demain

Emmanuel DAOUD, Solène SFOGGIA, Guillaume MARTINE et Hugo PARTOUCHE

136 | MENSUEL
AVRIL 2018

Wolters Kluwer

RLDA 6433

Prévention des risques, justice et nouvelles technologies : comment se préparer au droit pénal des affaires 3.0 ?

Par Emmanuel DAOUD
Avocat au Barreau de Paris
Cabinet Vigo
Membre du réseau GESICA

Et Solène SFOGGIA
Avocate au Barreau de Paris
Cabinet Vigo
Membre du réseau GESICA

Algorithmes, *blockchain*, *Big Data*, Internet des objets, les nouvelles technologies se diffusent partout. Si elles sont beaucoup moins élaborées que ce que l'on veut bien croire aujourd'hui, la vitesse de leur développement nous oblige à anticiper les transformations – majeures – qui se préparent.

Pour s'en convaincre, jetons un regard sur les décennies qui viennent de s'écouler : l'âge de l'ordinateur en 1950-1970, celui du logiciel en 1970-1990, des réseaux en 1990-2010, et désormais celui de la donnée, ont contribué, avec une rapidité qui n'en finit pas de nous surprendre, à un nouveau monde[1].

Si l'effervescence règne dans le secteur économique, notamment avec le lancement par le Premier ministre d'une stratégie nationale pour l'intelligence artificielle[2], le droit pénal des affaires, et plus largement le droit pénal, restent étonnamment à l'écart de ces innovations technologiques. Les protagonistes du moment ne s'en cachent pas : le droit pénal est trop sensible pour que ces technologies s'y intéressent – du moins pour le moment[3]. C'est ainsi le cas de *Caselaw*, qui affiche ouvertement ses réticences à l'égard du droit pénal, pour des raisons éthiques, craignant par exemple que les algorithmes permettent à terme de choisir la juridiction la moins sévère pour commettre une infraction[4].

C'est bien là tout l'enjeu de ces nouvelles technologies : elles bouleverseront certainement nos sociétés, et leur utilisation pose indéniablement un grand nombre de questions éthiques et philosophiques. Inscrit dans le cadre de ces réflexions, l'objet du présent article se veut aussi pragmatique : à quoi va ressembler l'entreprise de demain ? Quels seront les risques pénaux auxquels elle devra faire face ? Quelle stratégie peut-elle d'ores et déjà mettre en place pour les prévenir, et plus largement anticiper une justice pénale 3.0 ?

En réalité, certaines de ces technologies font déjà partie de notre quotidien, par exemple, les algorithmes utilisés par nos réseaux sociaux pour nous présenter le contenu le plus susceptible de nous intéresser. L'Internet des objets se développe, quant à lui, par la connexion de différents objets intelligents, pouvant interagir les uns avec les autres, pour développer de nouvelles applications ou services[5]. Parmi les dernières technologies particulièrement médiatisées, l'on retrouve aussi la *blockchain*, qui peut être définie comme une technologie de stockage et de transmission d'informations. Elle constitue ainsi une sorte de base de données, réputée sécurisée, et partagée entre ses différents utilisateurs, sans intermédiaire. Ses appli-

(1) F. Pellegrini, Intelligence artificielle, mégadonnées et gouvernance, RLDI 2018/144, n° 5152, p. 56-59.

(2) Lancement de la mission « Stratégie nationale sur l'intelligence artificielle », 8 sept. 2017, v. sur : <https://www.numerique.gouv.fr/economie-numerique-inclusion-numerique/lancement-de-la-mission-strategie-nationale-sur>.

(3) B. Barraud, La justice prédictive et la défense assistée par ordinateur : progrès ou menaces pour le métier d'avocat ? D. avocats, Exercer et entreprendre 2016, p. 374.

(4) C. Fleuriot, L'intelligence artificielle va provoquer une mutation profonde de la profession d'avocat, D. actualité, 15 mars 2017.

(5) L. Arcelin, Internet des objets et régulation, RLC 2016/55, n° 3078, p. 51-58.

cations sont diverses, de la cryptomonnaie aux contrats « intelligents » ou *smart contracts*[6].

Si cet article n'a pas vocation à énumérer toutes les technologies en germe, sans même évoquer celles qu'il reste à inventer, il n'en reste pas moins que les contours du droit pénal des affaires 3.0 peuvent être esquissés, à la lumière de ses principaux enjeux pour les entreprises et leurs conseils.

I. — La transformation de l'entreprise et de sa stratégie de prévention du risque pénal

La prévention des risques suppose en premier lieu de s'intéresser de plus près aux transformations de l'entreprise induites par la technologie, afin d'en tirer d'humbles pistes de réflexion, que l'entreprise peut d'ores et déjà appréhender.

A. — Quels impacts de la technologie sur l'entreprise et sur ses risques ?

Si les transformations que connaît l'entreprise dépendront nécessairement de son secteur d'activité et de son métier, leur ampleur est certaine, comme l'on peut déjà le constater en matière de santé, d'assurance, ou encore de finance[7].

Au niveau opérationnel, le développement de ces technologies devrait permettre d'automatiser et d'optimiser, de manière constante, les processus mis en œuvre. Ainsi, les objets connectés sont désormais capables de communiquer entre eux et de s'adapter automatiquement et continuellement en fonction des données échangées[8]. À cela s'ajoute le développement des algorithmes apprenants (ou *machine learning*), qui permettent à la machine d'apprendre, peu à peu, par elle-même[9]. La logistique offre un bon exemple de l'impact de ces technologies : des capteurs sont déployés, connectés aux véhicules (bientôt complètement autonomes ?) et marchandises, afin d'optimiser la visibilité et la traçabilité tout au long de la chaîne d'approvisionnement, en prenant en compte automatiquement d'éventuels changements de conditions (trafic, température, lumière, etc.). Les opérations de transport sont ainsi améliorées, adaptées automatiquement en fonction des flux de données échangés, permettant par exemple de réduire les risques de retard ou d'avarie.

Ces technologies s'accompagneront également inévitablement d'un gain de temps important pour certains métiers : ainsi, l'intelligence artificielle permettra, par exemple au sein du service juridique, d'analyser des milliers de documents et de données en une fraction de seconde, mais aussi d'établir plus rapidement des documents juridiques (notamment les contrats, statuts ou lettres) et de réaliser automatiquement certaines activités chronophages (tri, recherches juridiques, etc.), de manière de plus en plus pertinente[10].

Au niveau décisionnel, elles devraient aussi servir à soutenir et améliorer les processus de décision. Par exemple, une équipe de chercheurs britanniques et américains a construit un algorithme capable de prédire des décisions de justice huit fois sur dix, en croisant les faits, les arguments utilisés et le droit en vigueur[11]. Ainsi, le recours à l'intelligence artificielle permettra aux juristes d'évaluer les chances de succès de telle ou telle action, de proposer les arguments les plus adaptés, et de façonner la stratégie contentieuse sur la base d'un grand nombre de données[12].

Sur cette toile de fond, les risques essentiels de l'entreprise se dessinent assez nettement, au premier rang desquels figurent les risques techniques. Ces derniers peuvent être divisés en quatre catégories : (i) la violation de la confidentialité des données (pillage informationnel, divulgation accidentelle ou illicite, etc.), (ii) la violation de l'intégrité des données (altération, modification accidentelle ou illicite, etc.), (iii) la violation de la disponibilité des données (perte, destruction accidentelle ou illicite, etc.), et (iv) les atteintes aux systèmes d'information de l'entreprise (infection virale, destruction physique, bombe logique, déni de service, etc.)[13]. Statistiquement, il est intéressant de noter que les entreprises sont, déjà aujourd'hui, confrontées à plus de 1 500 menaces malveillantes chaque mois, et qu'au moins 80 % des infractions en matière de cybercriminalité sont le fait de salariés, anciens ou actuels[14].

À ce titre, l'entreprise s'expose à voir sa responsabilité pénale engagée dès lors que le salarié peut accéder à des fichiers professionnels de données à caractère personnel

(6) J. Deroulez, Blockchain et preuve, D. avocats, Exercer et entreprendre 2017, p. 58.

(7) G. Marraud des Grottes, Intelligence artificielle : la Cnil appelle à une plus grande vigilance, Actualité Du Droit, Wolters Kluwer France, Tech & Droit, déc. 2017.

(8) L. Arcelin, Internet des objets et régulation, RLC 2016/55, n° 3078, p. 51-58.

(9) G. Marraud des Grottes, Intelligence artificielle : la Cnil appelle à une plus grande vigilance, préc.

(10) B. Barraud, La justice prédictive et la défense assistée par ordinateur : progrès ou menaces pour le métier d'avocat ?, D. avocats, Exercer et entreprendre 2016, p. 374.

(11) B. Barraud, La justice prédictive et la défense assistée par un ordinateur : progrès ou menaces pour le métier d'avocat ?, préc.

(12) S. Larrière, Confier le droit à l'intelligence artificielle, le droit dans le mur ?, RLDI 2017/134, n° 4946, pp. 38-40.

(13) P. Lubet et S. Cullafroz-Jover , La souplesse du droit face à l'usage croissant du BYOD : Étude sur la gouvernance des données au sein de l'entreprise connectée, Revues des Juristes de Sciences Po n° 10, mars 2015.

(14) J.-B. Auroux, Nouvelles technologies de la communication électronique et droit pénal, RLDI 2006/15, n° 458, pp. 76-79.

depuis un environnement informatique non sécurisé [15]. Ces situations sont bien souvent régulières en pratique, comme l'accès au réseau de l'entreprise depuis un équipement nomade personnel vulnérable ou le transfert des fichiers de l'entreprise dans un espace de stockage en ligne ne présentant pas les modalités de protection adéquates [16]. Dans un contexte de production croissante des données, les articles 323-1 et suivants du code pénal ont en outre été continuellement adaptés, depuis leur introduction, afin de sanctionner les atteintes aux systèmes de traitement automatisé des données. À ce titre, la Cour de cassation a récemment jugé que le délit d'accès frauduleux à un système de traitement automatisé de données était caractérisé, dès lors que le praticien hospitalier, qui invoquait, pour se défendre, qu'il avait accédé aux ordinateurs de ses collègues uniquement pour rechercher des courriels susceptibles de lui être utiles dans le cadre d'un litige, n'avait pas l'autorisation de détenir le *keylogger* utilisé, en violation de l'article 323-3-1 du code pénal [17].

> *Si l'entreprise produit un nombre exponentiel de données, celles-ci constituent naturellement autant de preuves pouvant être utilisées en faveur ou contre l'entreprise.*

En outre, ces nouvelles technologies devraient aussi pouvoir, à l'instar d'Internet, offrir une nouvelle dimension aux infractions les plus classiques, le chantage, l'extorsion de fonds [18], ou même l'homicide, à supposer par exemple qu'un objet connecté défaillant ou piraté exécute un ordre ayant pour conséquence de tuer quelqu'un. En parallèle, l'entreprise devra aussi veiller à ce que les algorithmes qu'elle utilise n'aboutissent pas à discriminer ou harceler ses salariés ou ses clients ; ou puissent être utilisés dans ce sens.

A contrario, l'on peut penser que ces technologies permettront de réduire les occurrences de certaines infractions plus « classiques », grâce à la fiabilité et à la surveillance qu'elles induisent [19]. En effet, la technologie permet de monitorer en continu les comportements, habitudes et flux, de mieux détecter les fraudes, voire d'imposer des *process* afin de prévenir d'éventuels risques existants [20]. L'exemple des voitures sans chauffeur est parlant : des voitures conduites par des robots, sans émotion, sans fatigue, sans alcool et sans drogue – et donc sans accident [21] ? L'on peut aussi faire le parallèle avec la fraude fiscale ou le blanchiment, qui pourraient s'avérer plus complexes à dissimuler, compte-tenu de la combinaison de ces nouvelles technologies avec le renforcement des obligations de transparence et de vigilance pesant sur les acteurs économiques.

B. — Quelle stratégie de prévention des risques peut-on d'ores et déjà mettre en place ?

Dans ce contexte, la stratégie de prévention du risque pénal au sein de l'entreprise peut d'ores et déjà être façonnée autour de trois axes.

En premier lieu, l'entreprise devra nécessairement être en mesure, sur le plan technique, d'assumer la responsabilité structurelle de plus en plus lourde qui sera la sienne [22]. À ce titre, l'attention de l'entreprise devra non seulement porter sur le bon fonctionnement et la maintenance de chaque technologie, mais aussi sur leur fonctionnement global, compte-tenu de l'interconnexion croissante de ces technologies.

En pratique, cela fera peser sur la direction des systèmes d'information une responsabilité non négligeable, puisque l'entreprise devra démontrer qu'elle a pris l'ensemble des précautions techniques nécessaires, mis en place une organisation humaine et matérielle adaptée, et procédé à des maintenances, contrôles et audits réguliers. D'ores et déjà, il est intéressant de noter que les mesures de sécurité mises en place par l'entreprise ont pu avoir une répercussion directe sur l'appréciation portée par le juge sur les différents éléments constitutifs des infractions dont l'entreprise a été victime. Ainsi, la cour d'appel de Paris [23] a considéré, dans un cas où une entreprise s'était constituée partie civile en raison d'un accès frauduleux à son système de traitement automatisé des données, que la possibilité d'accéder à des données stockées sur un site avec un simple navigateur, alors qu'il y avait de nombreuses failles de sécurité, n'était pas répréhensible [24]. En

(15) P. Lubet et S. Cullafroz-Jover, La souplesse du droit face à l'usage croissant du BYOD : Étude sur la gouvernance des données au sein de l'entreprise connectée, préc.

(16) P. Lubet et S. Cullafroz-Jover, préc.

(17) Cass., crim., 16 janv. 2018, n° 16-87.168, P+B.

(18) J.-B. Auroux , Nouvelles technologies de la communication électronique et droit pénal, préc.

(19) D. Noguéro , Loi Badinter, voiture autonome, robot, évolution du risque et information au regard de la protection des assurés. Humble essai de projection sur les rails du futur, RLDI 2017/142, n° 5108, pp. 57-65.

(20) D. Noguéro , Loi Badinter, voiture autonome, robot, évolution du risque et information au regard de la protection des assurés. Humble essai de projection sur les rails du futur, préc.

(21) D. Noguéro, préc.

(22) P. Lubet et S. Cullafroz-Jover, La souplesse du droit face à l'usage croissant du BYOD : Étude sur la gouvernance des données au sein de l'entreprise connectée, préc.

(23) CA Paris, sect. A, ch. 12, 30 oct. 2002, n° RG : 02/04867, Antoine C. c/ Ministère public, SA Tati.

(24) J.-B. Auroux, Nouvelles technologies de la communication électronique et droit pénal, RLDI 2006/15, n° 458, préc.

d'autres termes, les éléments matériels et intentionnels de ces infractions dont l'entreprise pourrait être la victime seront d'autant plus faciles à caractériser que les mesures techniques mises en place par l'entreprise pour protéger son système seront développées.

En deuxième lieu, l'entreprise devra être capable de délimiter clairement les responsabilités de chaque intervenant. En effet, un nombre de plus en plus important de tiers a vocation à intervenir dans le fonctionnement quotidien de ces réseaux et technologies. Dès lors, en cas de défaillance technique, qui donnerait lieu à une action pénale de la victime, la responsabilité de l'entreprise pourrait être diluée aux côtés d'autres coauteurs. En effet, qui, de l'objet, de l'intelligence artificielle, de sa connexion, de son réseau ou encore de sa plateforme d'intégration devrait être tenu pour responsable[25] ? Si ces questions ne sont pas, en soi, nouvelles pour le droit pénal comme pour le droit civil, elles se complexifient en même temps que ces technologies. À ce titre, il convient de noter que la question de créer une personnalité juridique propre à l'intelligence artificielle n'est pas réglée, et est notamment sérieusement envisagée par le Parlement européen, à long terme, en matière de responsabilité civile[26].

Quelle qu'en soit l'issue, cette incertitude du droit positif doit interroger l'entreprise dans la mise en place de ces nouvelles technologies. Concrètement, la prévention du risque passera donc nécessairement par la mise en place de délégations de pouvoir en interne et la rédaction de contrats avec les différents intervenants, rigoureusement rédigés, afin d'assurer une définition claire des obligations et responsabilités de chacun[27].

Enfin, en troisième lieu, l'entreprise doit accompagner ce changement d'un nécessaire renforcement de sa fonction éthique. La CNIL recommande à juste titre, dans son rapport sur l'intelligence artificielle, de former à l'éthique tous les maillons de la chaîne algorithmique, de mettre en place un comité éthique, de diffuser des bonnes pratiques sectorielles ou encore de réviser les chartes de déontologie internes[28]. À ce titre, la CNIL insiste en effet sur le principe essentiel de loyauté des algorithmes, et ceux de vigilance et réflexivité, c'est-à-dire de questionnement régulier à l'égard de ces « objets mouvants », et de la responsabilité pouvant en découler pour l'entreprise qui les utilise[29].

In fine, l'on ne peut donc que conseiller aux services juridiques de se rapprocher, dès à présent, des services informatiques de l'entreprise, qui seront au cœur de la prévention du risque pénal de demain. Cette stratégie de prévention et d'autorégulation sera d'autant payante qu'elle constituera certainement l'un des axes de défense les plus solides pour l'entreprise dans le procès pénal 3.0.

II. — L'entreprise face à la justice pénale technologiquement assistée

L'introduction de ces nouvelles technologies dans le procès pénal, bien qu'elle se traduise par de réelles opportunités pour les juges comme pour les justiciables, ne se fera pas sans heurts – en particulier s'agissant de la protection des droits essentiels de la défense.

A. — Droits de la défense et nouvelles technologies : une équation impossible ?

Si l'entreprise produit un nombre exponentiel de données, celles-ci constituent naturellement autant de preuves pouvant être utilisées en faveur ou contre l'entreprise. Or, cette production croissante de données ne fera assurément pas bon ménage avec les nouvelles technologies d'enquêtes numériques – et les entreprises peuvent s'attendre à une vulnérabilité accrue face aux enquêteurs.

Ainsi, l'émergence de ce que l'on peut qualifier de véritables perquisitions numériques[30], dans un contexte d'Internet des objets[31], pourra permettre d'extraire un nombre inimaginable de données brutes, sans aucun contrôle de la part de l'entreprise. Cette vulnérabilité sera d'autant plus grande que l'entreprise n'en aura pas toujours conscience, par exemple avec la faculté nouvellement créée pour les enquêteurs de capter les données informatiques, à distance, à l'insu de l'intéressé[32] (notamment par l'article 706-102-1 du code de procédure pénale, restreint à certaines infractions).

Au même titre, l'enquête et l'administration de la preuve pénale seront bouleversés par les algorithmes. Ils permettent déjà de surveiller certaines activités, de retracer

(25) Entretien avec Laure de La Raudière, RLDC 2017/148, n° 6313, p. 40-43.

(26) Résolution du Parlement européen du 16 février 2017 contenant des recommandations à la Commission concernant des règles de droit civil sur la robotique (2015/2103(INL)).

(27) P. Lubet et S. Cullafroz-Jover, La souplesse du droit face à l'usage croissant du BYOD : Étude sur la gouvernance des données au sein de l'entreprise connectée, Revues des Juristes de Sciences Po n° 10, mars 2015.

(28) CNIL, Comment permettre à l'homme de garder la main ? Les enjeux éthiques des algorithmes et de l'intelligence artificielle, déc. 2017.

(29) CNIL, préc.

(30) O. Décima, Du piratage informatique aux perquisitions et saisies numériques ?, AJ pénal 2017, p. 315.

(31) C.-H. Boeringer, Points de Vue - État des lieux des visites inopinées, perquisitions et gardes à vue dans l'entreprise : l'enjeu de la saisie des données -Les nouvelles technologies rendent les sociétés plus vulnérables face aux enquêtes, Revues des Juristes de Sciences Po n° 10, mars 2015.

(32) M. Léna, Tableau récapitulatif des techniques d'enquête numériques judiciaires, AJ Pénal 2017, p. 169.

différents flux et montages financiers complexes[33] et devraient être capables prochainement d'analyser les pièces d'un dossier pénal afin d'en détecter chaque incohérence ou élément à charge, de déterminer la probabilité qu'une personne soit coupable ou non, ou encore d'évaluer la nécessité de placer une personne en détention provisoire au regard de son risque de fuite[34]. Le projet VALCRI, financé par la Commission européenne, est un bon exemple des applications en plein développement de ces technologies, avec l'analyse et la reconstruction de situations de crimes, permettant par exemple d'aider à en trouver l'auteur[35].

> *Ainsi, la blockchain pourrait permettre la mise en œuvre et le monitoring d'une peine de conformité, dans les conditions agréées par convention ou prévues par le jugement.*

À ce stade, l'une des technologies d'ores et déjà utilisée, quoique toujours en développement, réside dans *l'evidence based sentencing*, employée dans certains États américains. Il s'agit de l'utilisation d'un algorithme pour calculer la durée de la peine du condamné, censée minimiser son risque de récidive[36]. Ainsi, la Cour suprême du Wisconsin a utilité un algorithme pour condamner le prévenu à une peine de prison, sur la base du profil de risque établi par un algorithme secret, en dépit de toute idée de respect des droits de la défense, mais aussi du principe d'individualisation de la peine[37]. L'on notera en effet que cet algorithme n'a pas été dévoilé à la défense, qui n'a pu le contester : *quid*, pourtant, si cet algorithme intégrait par exemple l'origine du prévenu comme une variable d'analyse[38] ?

L'atteinte aux droits de la défense ne doit pas non plus être sous-estimée en raison du risque de déjudiciarisation et de dématérialisation de la procédure lié aux nouvelles technologies, en particulier dans le cadre d'un procès pénal attaché à son essence charnelle. Par exemple, le Royaume-Uni a initié depuis 2015 une réflexion sur les *online court*, c'est-à-dire la dématérialisation de la justice, mais uniquement pour les affaires civiles de faible importance. À terme, un logiciel devrait analyser le cas et proposer une solution, validée ou non par le juge[39].

En droit pénal, l'on peut penser que les droits de la défense, l'acceptation de la peine, et son utilité sociale, s'accommoderaient mal d'un verdict prononcé par un robot[40], quand bien même la justice serait plus rapide et plus économique. Si l'on est encore loin du magistrat robot, en France, où le dépôt de plainte en ligne vient seulement d'être créé[41], il est essentiel de rappeler que l'introduction des nouvelles technologies ne doit jamais faire écran entre le juge, le justiciable, et son conseil, dont le dialogue et la compréhension mutuelle sont essentiels dans une société démocratique.

À ce titre, il est intéressant de constater que des technologies plus anciennes nous ont prouvé à quel point il est trompeur de considérer la technologie comme un outil neutre, en particulier pour les droits de la défense[42]. On en veut pour preuve l'utilisation de la visioconférence, dont on constate que la justice n'a toujours pas pris la mesure[43], et dont le développement est d'ailleurs annoncé aux termes des Chantiers de la Justice du gouvernement[44]. Les enjeux liés à l'empreinte génétique, reine des preuves, sont également évocateurs, les avocats s'efforçant d'opposer une approche critique à l'expertise ADN[45], mettant l'accent sur ses possibles erreurs – bien souvent occultées – et refusant qu'elle constitue une preuve unique se suffisant à elle-même[46].

L'on ne peut donc qu'inviter le législateur à tirer profit de ces expérimentations, afin que la technologie ne se transforme pas en cimetière des droits de la défense mais soit, au contraire le support d'un principe du contradictoire et de droits de la défense renouvelés. En effet, de la même manière, avec ces nouvelles technologies, l'erreur est de considérer que leur usage serait neutre et sans biais : il est indispensable que l'entreprise et son avocat soient en mesure de discuter la fiabilité des données, la pertinence de l'algorithme utilisé, ou encore l'interprétation qui en est faite.

(33) B. Deffains, J.-B. Thierry, Les juristes rêvent-ils d'un droit algorithmique ?, Dalloz avocats, Exercer et entreprendre 2017, p. 392.

(34) K. Danielle, P. Guo, and S. Kessler, Algorithms in the Criminal Justice System : Assessing the Use of Risk Assessments in Sentencing. Responsive Communities Initiative, Berkman Klein Center for Internet & Society, Harvard Law School, 2017.

(35) Site internet de VALCRI, Visual Analytics for sense-making in criminal intelligence analysis : <http://valcri.org/about-valcri/>.

(36) B. Deffains, J.-B. Thierry, Les juristes rêvent-ils d'un droit algorithmique ?, préc.

(37) K. Danielle, P. Guo, and S. Kessler. Algorithms in the Criminal Justice System : Assessing the Use of Risk Assessments in Sentencing. Responsive Communities Initiative, préc.

(38) K. Danielle, P. Guo, and S Kessler, préc.

(39) M. Clément , Algorithmes au service du juge administratif : peut-on en rester maître ?, AJDA 2017, p. 2453.

(40) B. Barraud, Prospectif - Avocats et magistrats à l'ère des algorithmes : modernisation ou gadgétisation de la justice ?, Revue pratique de la prospective et de l'innovation, oct. 2017, dossier 11.

(41) Dossier de presse, Chantiers de la justice, mars 2018.

(42) J. Bossan , La visioconférence dans le procès pénal : un outil à maîtriser, RSC. 2011, p. 801.

(43) J. Bossan, préc.

(44) Dossier de presse, Chantiers de la justice, préc.

(45) C. Jean-Meïre , La preuve pénale, internationalisation et nouvelles technologies, La documentation française, Coll. Perspectives sur la justice, déc. 2007.

(46) P. Reviron , L'avocat à l'épreuve de l'ADN, AJ Pénal 2018, p. 73.

Concrètement, il sera donc nécessaire d'avoir accès de manière transparente à ces algorithmes, afin de s'assurer de la loyauté de la collecte de données, que sont écartées celles couvertes par le secret professionnel, qu'elles sont de qualité, et que les règles de calcul de l'algorithme sont loyales. Il est à ce titre inutile de préciser que cela n'ira pas sans une bonne connaissance technique de ces outils et de leur fonctionnement, pour l'entreprise comme ses conseils, mais aussi pour les juges, qui devront être sérieusement formés à l'utilisation de ces nouvelles technologies et à leur critique. En réalité, si un algorithme peut devenir de plus en plus intelligent par lui-même, il le devient seulement à la hauteur des données dont il a été nourri... et de leur qualité[47].

B. — De nouvelles peines en construction ?

Il ne sera pas ici question des peines futuristes, que nombre d'auteurs ont pu évoquer, comme les nouvelles drogues ou applications de réalité virtuelle permettant par exemple de simuler une peine de prison de milliers d'années, directement dans le cerveau de la personne condamnée, tandis que celle-ci ne durerait en réalité que huit heures[48]. La limite avec la torture n'est pas loin, pour ne pas dire dépassée, et l'on ne peut qu'espérer que la technologie, ici encore, ne se développera pas sans un solide garde-fou éthique.

Plus sérieusement, la technologie pourrait bien permettre de renforcer le principe d'individualisation et de diversification des peines, en permettant le développement de nouvelles formes de peine et de suivi. Par exemple, la peine de mise en conformité se développe en droit pénal des affaires, notamment avec la loi *Sapin II*, aux termes de laquelle l'entreprise peut être condamnée à mettre en place un programme de mise en conformité, sous le contrôle de l'Agence française anticorruption[49].

Or, le développement de la *blockchain* a ouvert de nombreuses perspectives, notamment en matière de « contrats intelligents » (ou *smart contracts*). Ces derniers sont en réalité des protocoles informatiques pouvant exécuter n'importe quel contrat et garantir l'exécution des obligations des co-contractants, dès lors que des conditions prédéterminées sont réunies[50], automatiquement, sans qu'aucun acteur n'intervienne. Par exemple, dans le cas d'un retard d'un train, le programme met en œuvre l'indemnisation automatique du voyageur. De même, dans le cadre d'une négociation commerciale, le programme peut prévoir l'envoi à partir d'une certaine date et à certaines conditions de documents ou de fonds[51].

Ainsi, la *blockchain* pourrait permettre la mise en œuvre et le *monitoring* d'une peine de conformité, dans les conditions agréées par convention ou prévues par le jugement. À défaut, le non-respect pourrait entraîner le versement automatique d'une amende, ou la suspension automatique de certains *process* au sein de l'entreprise.

En somme, comme bien souvent en droit, c'est la recherche de l'équilibre qu'il faut poursuivre dans la construction du droit pénal des affaires 3.0. Si ces nouvelles technologies permettent des avancées considérables qu'il nous appartient d'explorer, tant au sein des entreprises que du système judiciaire, elles interrogent et devront continuer d'interroger les juges, les entreprises et leurs avocats en termes de vulnérabilité aux risques, de droits de la défense et de libertés fondamentales[52].

Le souci d'efficacité de la justice ne doit pas être la seule raison d'être de ces technologies : leur développement doit aussi servir les droits de la défense et la qualité de la justice. La sincérité et la loyauté de la preuve, de même que les risques d'abus ou de biais dans l'utilisation des données et technologies doivent rester au cœur des préoccupations du législateur, des justiciables et acteurs du système judiciaire[53]. À cet égard, l'on ne peut donc que conseiller aux entreprises, à leurs juristes et avocats de se former au fonctionnement de ces technologies et de rapprocher leurs fonctions juridiques, éthiques et informatiques : il faudra comprendre pour oser, oser aller contre la technologie, convaincre le juge du revirement de jurisprudence ou du revirement... d'algorithme ? ■

(47) B. Deffains, J.-B. Thierry , Les juristes rêvent-ils d'un droit algorithmique ?, Dalloz avocats, Exercer et entreprendre 2017, p. 392.

(48) V. R. Andersen, Aeon, 13 mars 2014, Hell on Earth, disponible sur : <https://aeon.co/essays/how-will-radical-life-extension-transform-punishment>.

(49) art. 18, L. n° 2016-1691, 9 déc. 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique.

(50) J. Deroulez, Blockchain et preuve, D. avocats, Exercer et entreprendre 2017, p. 58.

(51) M. Mekki, Les mystères de la blockchain, D. 2017, p. 2160.

(52) C. Jean-Meïre , La preuve pénale, internationalisation et nouvelles technologies , La documentation française, Coll. « Perspectives sur la justice », déc. 2007.

(53) C. Jean-Meïre, préc.