Rapport de synthèse présenté par M. Le Professeur Guy DROUOT

« *La mémoire est l'art de conjuguer le souvenir et l'oubli* », Umberto Eco.

L'intérêt d'une table ronde comme celle-ci -et c'est l'esprit de toutes les tables rondes organisées par l'IREDIC depuis onze ans- est de permettre de croiser les regards sur un sujet d'une actualité brûlante. Regard des étudiants du Master de droit des médias et des télécommunications tout d'abord, qui ont mené des recherches approfondies sur des questions dont ils ignoraient à peu près tout il y a quelques mois encore. Regard des praticiens ensuite, avocat ou informaticien, qui ont enrichi le débat en apportant l'éclairage de leur expérience professionnelle. Regard des universitaires enfin, qui ont guidé et supervisé, sans chercher à en influencer le contenu, les travaux des étudiants.

Je tiens à remercier les uns et les autres pour leur précieuse contribution à l'étude d'un sujet peu ou pas encore abordé dans une Faculté de droit. Je remercie en particulier les étudiants dont les rapports sont aussi denses dans leurs contenus que riches dans leurs propositions.

A l'issue d'une journée d'échanges fertiles et une fois toutes leurs facettes analysées, le rapporteur ne peut pas ne pas se poser la question de savoir si les objets connectés ne sont pas, comme la langue d'Esope, « la meilleure et la pire des choses ». Trois grandes impressions peuvent se dégager, qui orientent les conclusions dans ce sens.

La première est que nous sommes en présence d'un véritable phénomène à la fois omniprésent . La seconde est que ce phénomène est particulièrement intrusif au regard de la vie privée. La troisième est que ce phénomène est porteur de menaces sur la sécurité des personnes. Enfin, la dernière est qu'il existe des garanties juridiques, mais que ces dernières sont largement perfectibles.

Un phénomène omniprésent.

Phénomène de mode ? Pas seulement. Le premier rapport (Koffi FIAWOO et Slim TOUHAMI), aborde les questions d'ordre technique : qu'entend-on par « Internet des objets ? », *IDO -IoT* pour l'acronyme anglais d'Internet of Things-. Une approche indispensable à la bonne compréhension du sujet, rappelant que les étapes du développement de l'IDO ont été parcourues en une poignée de décennies, depuis le web 1.0 jusqu'au web 3.0 et ont connu une explosion à la faveur de l'interactivité entre la machine et son utilisateur, mais également entre machines elles-mêmes (M2M). Un objet d'usage quotidien doté d'un capteur, relié au réseau par le wifi ou le Bluetooth, un hébergeur, les ingrédients permettant la mise en œuvre du dispositif sont réunis. De l'automobile à la brosse à dents, du réfrigérateur aux chaussures de sport, du bracelet au biberon, les objets connectés sont de plus en plus nombreux. L'on est loin des premières connexions appliquées aux ordinateurs, smartphones ou tablettes tactiles. Les objets échangent des contenus entre eux (par exemple dans le système IOS d'Apple), livrent également des informations à l'utilisateur, mais aussi aux tiers... Selon les prévisions de l'IDATE, près de 80 milliards d'objets seront connectés à l'horizon 2020, soit dans à peine cinq ans. En raison de leur multiplication, on passe inévitablement de l'Internet *des* objets à l'Internet de *tous* les objets. Nul ne peut alors se soustraire à ce phénomène.

Les objets connectés sont consommateurs de fréquences hertziennes. D'où les difficultés relevées en droit des réseaux (rapport Clara ALCOLEA, Caroline JUILLET et Myriam KITAR). Avec le trafic mobile, les objets connectés contribuent fortement à l'augmentation des besoins en fréquences, aggravant de ce fait la pénurie caractéristique au secteur. Dans la perspective de la conférence internationale de l'UIT qui doit se tenir en 2015, le rapport Toledano, commandé par la ministre en charge de l'économie numérique et remis en juillet 2014, préconise une « gestion dynamique du spectre », à l'instar de ce qui est fait aux États-Unis et au Royaume-Uni, pionniers en ce domaine. Non moins importante est la question des adresses IP, indispensables aux fonctionnement des objets connectés, également menacées de manière imminente de saturation (notamment la norme

IPv4). Une proposition de loi déposée en 2014 préconise la migration de tous les objets connectés vers l'IPv6, capable de supporter une quantité colossale d'adresses, donc de satisfaire les appétits de ces objets.

Dans le domaine de la propriété intellectuelle (rapport Ingrid ESTELLON, Cécile GEISTEL et Audrey WOUESSI-DJEWE), on s'interroge sur l'opportunité d'adapter les règles existantes à l'Internet des objets. L'objet connecté peut-il dès sa création être protégé par le droit des brevets ou le droit des marques ? La pratique du *Patent Troll,* courante aux États-Unis, peut se révéler un obstacle à la créativité si le brevet n'est pas utilisé. Certains objets, comme l'imprimante 3D ou la caméra *meMini* constitueraient des menaces pour le droit de reproduction et le droit de représentation. Enfin, les objets connectés constituent des proies idéales pour les contrefacteurs. On note que la contrefaçon affecte jusqu'à 10% du commerce mondial, il n'est donc pas surprenant qu'en parallèle, se développe un marché noir des objets connectés.

Les objets connectés sont multiples et variés, ils imprègnent la vie professionnelle et, dans la vie privée, marquent désormais le moindre de nos gestes quotidiens.

Le recours à ces objets par les entreprises est de plus en plus répandu : des lunettes connectées -les fameuses *Google Glasses*- des contrôleurs de la SNCF aux vêtements connectés que portent certains salariés -les *Wearables*- (v. Le rapport Audrey ALBAGLY et Anaïs JOSEPH-GABRIEL). Dans ce secteur, les chiffes cités sont éloquents : plus de 60% des objets connectés existants ont été achetés par les entreprises à des fins professionnelles. Dans le secteur des drones, un coup d'arrêt vient cependant d'être donné aux États-Unis par la *Federal Aviation Administration* au projet de drones de livraison initialisé par Google et Domino's Pizza. La FAA souhaite en effet imposer de nombreuses restrictions -obligation pour le pilote d'avoir en permanence l'appareil dans son champ de vision ou interdiction de voler au-dessus des gens-, totalement incompatibles avec la logistique d'une livraison.

Les objets connectés sont massivement utilisés dans le domaine de la santé, au point de parler aujourd'hui de « e-santé » ou de « consultation 2.0 ». La réalité rattrape la fonction (voir le film d'animation « Les nouveaux héros » de Don HALL et Chris WILLIAMS, où le robot infirmier *Baymax* est capable de diagnostiquer jusqu'aux états d'âme des patients). Les objets sont multiples, plus ou moins utiles, il est vrai : tensiomètre, pèse-personne, brosse à dents, patch, lecteur de glycémie, moniteurs divers... En attendant les implants qui feront de l'être humain lui-même une personne connectée. Le droit de la santé s'en trouve naturellement bousculé, notamment pour ce qui est du secret des données médicales. Le *Quantify Self* qui permet de mesurer les activités physiques à chaque instant, constitue une sérieuse source d'atteinte à la vie privée (rapport Léonor CHOUX, Lauren ESTRUCH et Sandrina GONÇALVES).

Les premiers impactés sont les utilisateurs eux-mêmes. L'approche par la sociologie des usages, (rapport Éloïse FLORENT, Marine MANCEAU et Manon RAMAGE), nous apprend que les possesseurs des objets connectés sont majoritairement des hommes appartenant aux CSP supérieures et vivant en région parisienne. La majorité des utilisateurs estime que ces objets facilitent la vie quotidienne (les parents de nouveaux-nés, les personnes âgées, les sportifs...), sont un facteur de socialisation, mais paradoxalement qu'ils favorisent l'isolement, la discrimination et induisent le contrôle social, voire la déshumanisation. Il est vrai que les objets connectés les plus utilisés concernent la puériculture, la santé, l'habitat, l'électroménager, les sports. Autant dire toutes les étapes et toutes les facettes de la vie quotidienne de l'homme. Au-delà, se pose la question du rapport de l'homme à la machine : l'homme reste-t-il toujours maître de la machine ou commence-t-il à être asservi par elle ? Le risque d'addiction, évoqué par les auteurs, est loin d'être négligeable.

Le second impact est d'ordre économique (rapport Célia CERVERA, James HAILLON et Benjamin LESIRE-OGREL). Les chiffres cités sont vertigineux et témoignent d'un essor économique et commercial fulgurant. L'offre diversifiée, s'appuyant sur une force de frappe commerciale redoutable, se déploie sur un marché pluriel mettant en concurrence les *start up* et les grand

groupes industriels. Dans ce secteur, comme dans celui du numérique en général, l'on passe rapidement de la phase de « l'économie de garage » à celle de la mondialisation. Il existe cependant des freins sérieux au développement du marché : le coût et le côté « gadget » des objets, les problèmes d'interopérabilité/compatibilité, les craintes inhérentes aux menaces sur la vie privée, les failles de sécurité affectant 70% des objets, etc. La discussion qui s'ensuit fait apparaître que les paradigmes classiques de la science économique sont sérieusement bousculés par l'apparition des objets connectés, au point de susciter l'émergence de paradigmes nouveaux.

L'utilisation des objets connectés présente un côté ludique indéniable. Conviviaux, intuitifs, nomades, ergonomiques, esthétiques de surcroît, ces objets possèdent de nombreux atouts pour séduire le consommateur *geek*. Mais ce dernier est-il conscient des risques induits par leur utilisation ?

Un phénomène intrusif au regard de la vie privée.

Le pouvoir intrusif des objets connectés pose une question fondamentale : *existe-t-il encore une sphère privée ?* C'est la question à laquelle s'efforcent de répondre les auteurs du rapport sur les données personnelles (Margot GEITNER, Laura KASSAIAN et M. Sébastien HERAUD). Avec la diffusion massive de ces données, l'anonymat et le secret de la vie privée s'estompent derrière la « désanonymation ». Dans quelle mesure est-ce légal ? Lors de son Forum de décembre 2014, le G29 -réunion des CNIL européennes- a identifié les menaces pesant sur les données personnelles et rappelé que les objets connectés étaient soumis au respect du droit européen. En effet, la vulnérabilité des données personnelles face à ces technologies ne laisse pas d'inquiéter. La pratique, très en vogue, du *Data Mining*, souvent présentée comme une panacée dans le monde de l'entreprise, peut donner lieu à des dérives telles que le piratage des contenus ou l'usurpation d'identité facilités par l'insuffisance des contrôles. Les campagnes de sensibilisation lancées par la CNIL suffiront-elles à amorcer une prise de conscience ? Les initiatives publiques communautaires -*Privacy by Design, Privacy by Default, Accountability, Privacy Impact Assessment*) ou nationales, sont parfois complétées par les initiatives privées, avec l'adoption de chartes ou de codes de bonne conduite.

Du côté de l'entreprise, les apports de l'IDO sont indéniables en termes de rentabilité et d'ergonomie (rapport Audrey ALBAGLY et Anaïs JOSEPH-GABRIEL). En droit du travail, les objets connectés sont même utilisés dans des procès en responsabilité civile, pour le calcul des indemnités, comme l'atteste le cas du bracelet *Fitbit* dans des contentieux jugés au Canada ou aux États-Unis. Mais il y a le revers de la médaille, comme le montre l'exemple révélateur de l'entreprise Yahoo, qui a mis gracieusement a la disposition de son personnel des bracelets connectés leur permettant d'accéder à leur courriel, SMS, agenda, téléphone portable, album de photos, ainsi que les données de santé. Un accès ouvert également à l'employeur... Quant à la géolocalisation du salarié, il est rappelé qu'elle n'est autorisée que si elle est justifiée par la nature de la tâche à accomplir et proportionnée au but recherché.

Sur le plan judiciaire, Me Nicolas COURTIER rappelle que les toutes premières applications contentieuses de ce que l'on n'appelait pas encore « objets connectés » remontent à l'affaires OM/VA où un badge d'autoroute avait servi de preuve à décharge (1993), et à l'assassinat du Préfet Érignac à l'occasion duquel la localisation des téléphones mobiles avait permis de confondre les suspects (1998). Il souligne que si les affaires plaidées sont actuellement limitées, elles concerneront surtout, à l'avenir, les contrats commerciaux, mais aussi les atteintes au secret de la vie privée. Les contentieux à venir ne tarderont pas à se multiplier dans de nombreuses branches du droit. On peut citer par exemple la jurisprudence naissante à propos de l'usage illicite des drones (v. *Infra*).

En droit de la santé, c'est le secret médical qui est mis à mal et qui met en évidence la nécessité d'encadrer l'utilisation des données de santé. Ces dernières ont été qualifiées de sensibles par la directive européenne 95/46/CE. Or, c'est l'usage abusif des objets connectés par les utilisateurs

qui met en danger ces données, au point de susciter l'inquiétude de la CNIL (rapport Léonor CHOUX, Lauren ESTRUCH, Sandrina GONÇALVES).

N'a pas été évoqué le risque que présente au regard de la vie privée, le survol par les drones de zones habitées ou de propriétés privées. Or, la majorité des drones grand public commercialisés sont équipés de dispositifs de prise de vues (caméras ou appareils photographiques embarqués).

Un phénomène porteur de menaces.

Il s'agit d'abord des menaces sur la sécurité physique des personnes. Ces menaces sont identifiées à propos des accessoires de santé (déconnexion de pacemaker, de pompe à insuline, etc.). Les automobiles connectées ont été pointées du doigt aux États-Unis. Dans un rapport rendu public en février 2015 (« *Tracking & Hacking : security & privacy gaps put american drivers at risk* »), le sénateur démocrate Ed MARKEY dénonce les failles de sécurité présentes dans les véhicules connectés de 16 grandes marques. Ces failles, qui affectent presque 100% des voitures connectées, permettent à n'importe quel pirate d'en prendre le contrôle, provoquer un accident ou simplement recueillir les données sur le parcours suivi. On peut estimer que ce genre de menace est exponentiel dans la mesure où le nombre de voitures connectées devrait passer de 36 millions d'unités aujourd'hui à 152 millions en 2020.

Menaces ensuite sur les droits des personnes. Dans le monde du travail, les apports positifs des objets connectés sont loin de compenser les menaces pesant sur les employés : espionnage des salariés, géolocalisation, harcèlement, pressions diverses. L'actualité de ces derniers mois a montré que des salariés d'Apple Retail avaient fait l'objet d'une surveillance à leur poste de travail au moyen des caméras de vidéosurveillance, ce qui a valu à société un rappel à l'ordre par la CNIL (décision du 14 octobre 2014). L'objet connecté se transforme en effet en « boîte noire » du salarié. Il accompagne désormais son parcours professionnel, depuis l'entretien d'embauche jusqu'au licenciement, en passant par l'exécution du contrat de travail. Signe des temps, une nouvelle pathologie du travail apparaît : le *technostress*, engendré par un environnement à tout le moins suspicieux et propice au harcèlement numérique.

Menaces également sur certains aspects des droits d'auteur. Nous apprenons ainsi que l'utilisation des imprimantes 3D est susceptible de porter atteinte au droit de reproduction de l'auteur, et que la caméra *meMini* peut menacer le droit de représentation (rapport Ingrid ESTELLON, Cécile GEISTEL et Audrey WOUESSI-DJEWE).

S'agissant de la sécurité des sites sensibles, l'on rappellera simplement les survols répétés par des drones, depuis l'automne 2014, de sites tels que les centrales nucléaires, la base de sous-marins de l'Ile Longue dans la rade de Brest, le palais de l'Élysée, l'ambassade des États-Unis, etc. Des condamnations ont déjà été prononcées par les tribunaux pour mise en danger de la vie d'autrui et non respect de la réglementation aérienne (par ex. TGI de Nancy, Ordonnance d'homologation 20 mai 2014, Ministère Public / M. T.).

L'intervention du Professeur François PELLEGRINI enrichit le débat en insistant sur l'enjeu majeur que représente la sécurité et en proposant des pistes de réflexion. Parmi celles-ci les réseaux MESH, ou réseaux maillés (utilisés notamment en Syrie et en Égypte, lorsque le gouvernement a coupé les réseaux au début de la contestation), qui offrent le possibilité d'échapper à la cybersurveillance, en contournant les opérateurs.

Existe-t-il des parades ? En tout état de cause, elles seraient dérisoires car, selon les experts, il est impossible de doter chaque objet connecté d'un système de sécurité.

Des garanties juridiques existantes mais largement perfectibles.

Les garde-fous juridiques ne manquent pas, tant dans le droit français que dans le droit communautaire. Les rapporteurs ont cité le socle que constituent la loi Informatique, fichiers et libertés du 6 janvier 1978 et la directive 95/46/CE. Cette dernière, devenue obsolète, fait l'objet d'une réactualisation. Un projet de règlement initié par Viviane Reding, alors commissaire européen, a été approuvé par la Commission, ainsi que par le Parlement, mais le Conseil doit encore se prononcer.

Viennent ensuite les textes spécifiques, tels les codes : code de la santé publique, code du travail, code des transports, code de la propriété intellectuelle, code des postes et des communications électroniques. Ces textes méritent un toilettage justifié par la multiplication des objets connectés. Puis viennent les textes spécifiques, adoptés pour l'encadrement de ces objets : la loi du 28 mars 2014 relative à la géolocalisation, les arrêtés du 11 avril 2012 relatif à l'utilisation de l'espace aérien par les drones, pour ne citer que ceux-là.

Aux États-Unis, le *Children's Online Privacy Protection Act* (COPPA) de 1998 vise à protéger la vie privée des enfants sur Internet.

Un sujet n'a cependant pas été abordé au cours de cette journée : celui des applications militaires de l'IDO. Certes, il n'entrait pas dans le champs de recherche proposé au départ, mais rien n'empêche d'y faire une brève allusion. Les armées recourent très largement aux objets connectés, notamment en matière d'armement, dans un contexte conflictuel. Tel est le cas des équipements *high-tech* dits « de tête » équipant les pilotes d'avions, comme le casque du type *Look & Shoot* permettant d'atteindre quasi-instinctivement plusieurs cibles à la fois, en « effaçant » la carlingue de leur propre avion du champ de vision. Tel est encore le cas des drones armés, qui bouleversent les schémas classiques des conflits, notamment celui des guerres asymétriques.

Alors *Must* ou pas ? L'IDO se présente comme Janus. Une face avec les avantages qu'il procure, le progrès qu'il apporte, le modernisme qu'il incarne. Une face avec les inconvénients qu'il comporte, les menaces dont il est porteur, les dangers qu'il induit. Ainsi que le suggère la Professeure Dominique Augey, il ne faut pas limiter l'usage des objets connectés aux personnes. Les usages publics, dans un but d'intérêt général, ne manquent pas, comme le montre l'exemple des villes intelligentes,

Guy Drouot
Professeur des universités à Sciences-po Aix