Lettre n°68 - Novembre 2017 - disponible sur omc.ceis.eu

TABLE DES MATIERES

L'ANALYSE FORENSIQUE A L'EPREUVE DE L'INTERNET DES OBJETS

L'analyse forensique numérique est le travail mené sur un système d'information pour extraire, conserver et, parfois interpréter l'ensemble des informations que l'on peut y trouver, essentiellement sur ses différentes mémoires (vives, mortes, caches), sur son fonctionnement – ou le plus souvent, sur un dysfonctionnement - actuel ou passé.

Elle peut avoir des objectifs différents, selon le cadre dans lequel elle est conduite : dans un cadre judiciaire, elle vise à collecter toutes les preuves légales et incontestables permettant d'identifier et de punir les auteurs d'un délit ou d'un crime (attaque informatique, vol de données, pédopornographie, et plus généralement, tout crime ou délit dont la commission a visé ou utilisé un système d'information, ou peut être prouvée par son analyse forensique). Dans le cadre de la sécurité des systèmes d'information, elle vise à collecter toutes les informations permettant de comprendre l'enchaînement des processus informatiques ayant conduit à un dysfonctionnement ou au succès d'une attaque et d'évaluer son impact, afin de prendre les mesures correctrices nécessaires pour restaurer la sécurité et la disponibilité du système, de ses processus et de ses données.

Le développement fulgurant de l'Internet des Objets modifie considérablement l'espace numérique. Dans les entreprises, où ces objets sont de plus en plus présents, le travail d'enquête et de réponse à incident se trouve grandement complexifié. D'une part, l'inventaire de la totalité des objets connectés est difficile à réaliser, d'autant qu'il est dynamique du fait de la mobilité de certains dispositifs. D'autre part, l'analyse et l'accès aux objets ayant potentiellement participé à l'incident de sécurité sont rendus difficiles par la diversité des interfaces.

Les objets connectés ont un intérêt certain pour les attaquants, et donc pour l'analyse forensique[1] : ils sont facilement oubliés dans l'inventaire des systèmes d'information, voire même inconnus de la direction informatique ; ils sont difficiles ou parfois même impossibles à mettre à jour en fonctionnement, quand – cas encore trop rares – leurs fabricants en corrigent les failles de sécurité ; nombreux sont ceux qui reposent sur des réseaux sans-fil[2]… Ils constituent ainsi des cibles de choix pour de potentielles attaques, qu'il s'agisse de les intégrer à un *botnet* pour lancer des attaques DDoS, de perturber leur fonctionnement pour nuire à l'entreprise, de dérober des données ou encore de servir de vecteur pour d'autres attaques, par exemple pour pénétrer dans le système d'information de l'entreprise (par exemple une ampoule connectée qui sera attaquée dans le but de dérober le code d'accès WiFi).

Comment l'Internet des Objets conduit-il à modifier le travail d'analyse forensique, et quelles pistes potentielles pour répondre à cette problématique ?

[1] On parle alors d'objets d'intérêt forensique (OOFI pour *Object of Forensic Interest*).

[2] Les récentes vulnérabilités relatives aux protocoles BlueTooth et WPA2 (WiFi) nous rappellent les problématiques liées à l'intégration au système d'information de dispositifs employant des connexions sans fil.

L’extension du périmètre de l’analyse forensique

Les informations permettant de comprendre l'origine d'un incident ayant concerné un objet connecté peuvent être contenues à divers endroits :

- Dans l'objet connecté à proprement parler ;
- Dans les dispositifs internes à l’entreprise qui offrent une connexion à l’objet connecté ;
- Dans des dispositifs externes à l’entreprise : Cloud, fournisseurs du réseau de transport des données (sigfox, GSM, etc.).

En outre, les objets connectés peuvent appartenir à différents types de réseaux :

- Des réseaux personnels, reliés ou non aux réseaux domestiques ou professionnels : ce type de réseau comprend par exemple un *smartphone*, une *smartwatch*, des dispositifs audio sans fil, etc. ;
- Des réseaux domestiques : ils peuvent comprendre les ordinateurs personnels et les dispositifs qui relèvent de la domotique, et sont en général connectés à Internet via une box Internet ;
- Des réseaux d’entreprise, auxquels sont de plus en plus souvent rattachés des éléments GTC/GTB[3]. Cela peut donc comprendre les thermostats connectés, l’éclairage intelligent, la gestion des accès physiques (systèmes de badges), les alarmes, etc. La dilution de la responsabilité de ces objets entre divers services peut aboutir à une mauvaise gestion des risques. Il est courant de voir le parc de caméras IP géré exclusivement par la direction sécurité, qui n’est pas forcément la mieux placée pour gérer la sécurité informatique de ces objets connectés.
- Des réseaux métropolitains, dont les points d’accès publics gratuits sont susceptibles d’être usurpés afin de piéger les utilisateurs non sensibilisés.

Du fait des équipements nomades, qui peuvent être amenés à se connecter successivement à tous les types de réseau précédemment cités, il y a une perméabilité entre ces réseaux. L’investigation numérique peut ainsi nécessiter de prendre en compte les déplacements des personnes, les connexions réalisées par leurs équipements, et donc les réseaux et autres objets auxquels ils ont été connectés : le lave-vaisselle ou l’écoute-bébé connecté de l’employé peut devenir un élément pertinent de l’enquête forensique.

Des difficultés organisationnelles d’accès aux données utiles à l’analyse forensique

La perméabilité des réseaux pose évidemment la question de l’accessibilité à ces objets connectés ou aux données issues de ces objets qui sortent du périmètre de l'organisme, à savoir ceux qui relèvent :

- De réseaux domestiques des collaborateurs ;
- De réseaux publics ouverts ;
- D’opérateurs réseaux ;
- D’éditeurs de solutions en Cloud.

En effet, de nombreux objets ne sauvegardent pas les données en local, mais les transfèrent vers un système externe, où elles sont exploitées. S’agissant des données stockées à l’extérieur (dans le Cloud, à l’étranger), l’accès peut être problématique. En-dehors des cas où l’éditeur souhaite coopérer (si le contrat le prévoit ou

[3] Gestion Technique du Bâtiment / Gestion Technique Centralisée.

si l'éditeur y voit un intérêt pour renforcer sa sécurité), il est très difficile d'obtenir un accès aux données. Plus la donnée demandée est de nature technique – log IP par exemple – plus l'éditeur pourra être enclin à les fournir. Cependant, la majorité des éditeurs se montreront hostiles à tout partage de données de contenus concernant des individus (carnets d'adresse, discussions, groupes secrets, etc.), alors qu'ils peuvent avoir un intérêt pour l'analyse forensique. Aux Etats-Unis par exemple, Amazon a refusé de remettre les données d'un Amazon Echo (assistant personnel) à la police américaine dans le cadre d'une enquête sur un meurtre, jusqu'à ce que le suspect lui-même demande à l'entreprise cette mise à disposition des données[4]. Difficile d'imaginer une meilleure coopération dans le cadre d'une réponse à incident informatique.

Des difficultés techniques d'accès aux données contenues dans les objets connectés

Damien Cauquil, responsable R&D chez Digital Security, explique qu'une grande partie des objets connectés posent des difficultés techniques dans l'accès aux données. Il est généralement beaucoup plus difficile de réaliser des copies exactes des données contenues dans les mémoires de nombreux objets connectés que pour les composants informatiques. Les experts forensiques doivent identifier les composants, réussir à s'interfacer et réussir à récupérer l'information sans l'altérer. Il relève plusieurs difficultés spécifiques aux objets connectés :

- L'accès physique aux puces peut être particulièrement difficile, car non prévu par les constructeurs.
- Les experts font face à une grande diversité de systèmes d'exploitation (OS), qui complexifie l'accès aux données contenues en local. Il n'y a pas encore d'OS standard ou leader comme peuvent l'être Windows/Linux/OS X pour les ordinateurs ou bien Android/IOS pour les *smartphones*[5]. En effet, les besoins en ressources des dispositifs étant très différents, bien plus que celles séparant les différents modèles de *smartphone*, les caractéristiques techniques le sont tout autant. Ces dernières sont tirées vers le bas, afin de diminuer les coûts et la consommation électrique (essentiellement pour des raisons d'autonomie). Pour cette raison, on ne peut pas envisager de système d'exploitation polyvalent qui pourrait piloter tout le panel des objets connectés, car un tel système tirerait au contraire vers le haut le besoin en ressources de calcul.
- Beaucoup de systèmes emploient un pilote d'exploitation (*driver*) mémoire spécifique : il va parfois falloir se tourner vers le constructeur pour connaître le formatage de la mémoire sur la puce : la méthode de *paging*, la position des données relevant du contrôle d'intégrité et celles qui contiennent les données exploitables, etc.
- La compromission de l'objet connecté a pu entraîner la destruction des interfaces d'administration. Ceci ne constituerait pas un frein dans le cas d'un serveur traditionnel, ou plusieurs méthodes matures permettent d'accéder aux données malgré la destruction de l'interface traditionnelle (KVM, accès facilité aux composants mémoire, etc.). Les constructeurs d'objets connectés ne prévoient

[4] http://edition.cnn.com/2017/03/07/tech/amazon-echo-alexa-bentonville-arkansas-murder-case/index.html

[5] Des acteurs majeurs développent cependant des systèmes d'exploitation dédiés aux objets connectés qui visent un panel aussi large que possible, mais ceux-ci ne représentent actuellement qu'une part de marché négligeable : *Brillo* pour Google, *RIOT* qui est issu de la recherche académique en France et en Allemagne, *mbed OS* Pour ARM, *Windows 10 IoT Core* pour Microsoft… On peut souhaiter une standardisation des systèmes d'exploitation par typologie d'objets connectés, mais celle-ci ne semble pas encore se dessiner.

généralement pas d'accès de secours, pas plus que des journaux d'événement, alors que c'est une pratique courante s'agissant des routeurs, pare-feu, etc.

Le nerf de la guerre : les journaux d'événements et la question de leur génération

Pour faire face à la complexification, des outils spécialisés émergent. OpenText développe *EnCase Mobile Investigator*, un outil de collecte et d'analyse de données forensiques dédié aux objets connectés (*smartphone*, *smartwatch*, dispositif GPS, tablette, drone, etc.), et qui prend en compte la problématique des données hébergées dans le Cloud par le fournisseur de services[6]. Cellebrite développe depuis 2007 l'*Universal Forensic Extraction Device* (UFED), qui permet l'analyse forensique de très nombreux appareils, notamment mobiles : *smartphones*, assistants personnels, téléphones cellulaires classiques, dispositifs GPS, tablettes, etc. L'entreprise a notamment fait parler d'elle lorsque le FBI a fait appel à elle pour accéder aux données du téléphone du tueur de San Bernardino[7]. Dans le cas des terminaux personnels (*smartphones*, tablettes, etc.), notons que la principale difficulté se situe effectivement du côté des systèmes de protection des données de l'utilisateur (*privacy*) : chiffrement, mots de passe, etc.

L'analyse des données forensiques présentes sur les objets connectés présente un niveau de difficulté différent selon le type d'objet, que l'on pourrait distinguer de la façon suivante :

- Les objets connectés dont les performances – capacité de calcul, mémoire vive et stockage – les rapprochent des ordinateurs traditionnels. Il s'agit des *smartphones*, des imprimantes professionnelles et dispositifs de puissance similaire ;
- Les objets connectés dont les capacités sont minimales.

Les premiers permettent d'intégrer des solutions de sécurité, parfois des solutions de détection et de prévention des menaces, mais surtout et *a minima* des journaux d'événement qui peuvent aider à l'investigation.

S'agissant des seconds, il faut s'intéresser aux flux réseaux échangés avec les objets connectés auxquels il est si difficile d'accéder directement. La sécurité de ces objets doit effectivement être assurée à leur périphérie, préférablement au plus proche, c'est-à-dire intégrée au niveau de l'interface où ces flux pénètrent dans le système principal. Cela peut se réaliser via un pare-feu applicatif ou des sondes réseaux reliées à un SIEM, qui généreront les *logs* que les objets ne créent pas par eux-mêmes. Les objets de faible capacité étant généralement connectés par connexion sans-fil, donc directement exposés à des attaques, il s'agit surtout de protéger le système d'information des menaces transitant par l'objet connecté, et non l'inverse.

[6] Le logiciel Encase est l'un des outils de référence dans l'analyse forensique en vue de produire des preuves numériques. Il s'agit ici d'une version spécifique dédiée à l'Internet des objets. Parmi les autres outils de référence, on peut citer *Forensic Toolkit* (FTK) de AccessData ou encore *Helix* de e-fense (anciennement une solution open-source gratuite).

[7] https://theintercept.com/2016/10/31/fbis-go-hackers/

Conclusion

Damien Cauquil relève que, malgré plusieurs cas avérés, les objets connectés[8] ne sont pour le moment que rarement exploités afin de s'introduire dans les systèmes d'information des entreprises.

Il ne fait cependant aucun doute que des attaques finiront par exploiter les vulnérabilités qu'apportent souvent les objets connectés aux systèmes professionnels auxquels ils sont connectés. Cela rend plus que jamais nécessaire de prévoir, dès la conception des systèmes, y compris des objets connectés, tout ce qui sera nécessaire pour en assurer efficacement la cyberdéfense, et au-delà, les analyses forensiques futures : des journaux d'événements aussi complets et pertinents que possible, les points les plus adaptés où mettre les sondes de détection, des interfaces permettant de lire toutes les mémoires et d'analyser l'activité des systèmes en fonctionnement). Il est capital de ne pas limiter la notion de *security-by-design* à la seule cyber protection : elle doit s'appliquer à la cyberdéfense, qui nécessite de disposer de *logs*. L'analyse forensique s'anticipe dès la conception de l'objet. Pour l'entreprise qui exploite des objets connectés, la cyberdéfense et les analyses forensiques futures doivent être anticipées avant l'intégration des objets connectés au système d'information : il faut définir les solutions et les architectures permettant d'assurer la traçabilité des événements et la meilleure protection possible du système d'information.

[8] Précisons que le CERT-Ubik (Digital Security) exclue de la définition d'objet connecté les smartphones et imprimantes connectées, des dispositifs au contraire très ciblés. On notera au passage que les imprimantes d'entreprise (à la différence des imprimantes grand public) génèrent beaucoup de *logs*, et disposent d'interfaces très complètes.

PREUVE NUMERIQUE ET VALEUR PROBATOIRE

Au sens large, la preuve numérique peut être définie comme toute information stockée ou transmise sous forme numérique et qui revêt une certaine valeur probatoire, c'est-à-dire qu'elle peut être utilisée pour prouver quelque chose. Ainsi, elle peut se présenter sous différentes formes (textes, images, vidéos, sons, code informatique, etc.) et provenir de nombreuses sources (ordinateurs, *smartphones*, tablettes, objets connectés, internet, etc.). La preuve numérique a généralement vocation à être utilisée dans une procédure judiciaire. Elle peut être définie par la loi, ou à défaut, la valeur probatoire d'une information numérique peut être déterminée par le juge ou par les parties à un contrat (clause contractuelle sur les preuves admissibles entre les parties).

Que ce soit au sens large ou au sens juridique, pour qu'une information numérique dispose d'une valeur probatoire, il faut pouvoir démontrer son intégrité. Or, une information numérique est un produit de la technique informatique et peut, à ce titre, être facilement déplacée, altérée, endommagée ou même détruite lors de son traitement. Se pose alors la question de la fiabilité de la preuve numérique : quelle confiance accorder à la preuve numérique ? Comment son intégrité est-elle assurée ?

Si la preuve numérique est reconnue juridiquement depuis longtemps[9], la valeur probatoire de l'information numérique se renforce avec l'utilisation croissante de techniques spécifiques garantissant l'intégrité de l'information numérique.

Le renforcement de la valeur probatoire de l'information numérique

Depuis quelques années, la valeur probatoire de l'information numérique est davantage reconnue juridiquement. Parallèlement, l'information numérique tend à être de plus en plus utilisée à une fin probatoire.

Le renforcement du cadre juridique

En France, le cadre juridique de la valeur probatoire de l'information numérique s'est renforcé depuis la loi du 13 mars 2000 portant adaptation de la preuve aux technologies de l'information et relative à la signature électronique. Ainsi, la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique[10] reconnaît la possibilité, dans le secteur public comme privé, d'apporter la preuve d'une identité par un moyen d'identification électronique qui est reconnu comme fiable jusqu'à preuve du contraire, lorsqu'il répond à un cahier des charges établi par l'ANSSI[11]. L'ordonnance n° 2016-131 du 10 février 2016 portant réforme du droit

[9] En France, la loi du 13 mars 2000 portant adaptation de la preuve aux technologies de l'information et relative à la signature électronique a reconnu la valeur probatoire de l'écrit sous forme électronique, "sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité" : https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000399095

[10] https://www.legifrance.gouv.fr/affichTexte.do;jsessionid=33F702073C5E08541E41E9F5D17FB879.tplgfr37s_3?cidTexte=JORFTEXT000033202746&categorieLien=id

[11] https://www.usine-digitale.fr/article/le-recours-aux-moyens-d-identification-numerique-s-ouvre-au-secteur-prive.N472683

des contrats, du régime général et de la preuve des obligations[12] est venue consacrer la notion de « copie numérique fiable » qui revête la même valeur probatoire que l'original[13]. Soulignons que d'autres pays européens comme la Belgique ou le Luxembourg reconnaissent également cette force probante de la copie numérique. Notons également que la législation fédérale américaine relative à la preuve a, de son côté, récemment été amendée pour introduire une présomption d'authenticité pour certains documents numériques (articles de presses, documents publics par exemple)[14].

Enfin, rappelons que le règlement eIDAS n° 910/2014 du 23 juillet 2014[15], qui a pour ambition d'accroître la confiance dans l'économie numérique au sein de l'Union européenne, a notamment pour objet (article premier du règlement) de fixer les conditions de la reconnaissance, par les autres États membres, des moyens reconnus à l'échelon national pour l'identification électronique des personnes physiques et morales et pour l'acceptation, en tant que preuve, de certaines informations électroniques comme les signatures électroniques, les documents électroniques ou l'horodatage[16].

L'utilisation croissante de la preuve numérique

Avec le développement d'internet et des objets connectés, l'information numérique est de plus en plus utilisée pour la manifestation de la vérité. Par exemple, les assureurs utilisent les publications sur les réseaux sociaux pour apporter la preuve d'une fraude à l'assurance ou le Big Data pour démontrer l'existence d'une fraude organisée dans les contrats d'assurance [17]. Les objets connectés peuvent être également utilisés comme un moyen de preuve. Au Canada, des avocats ont utilisé un bracelet connecté pour apporter la preuve en justice des dommages subis par leur cliente du fait d'un accident de voiture, afin obtenir une indemnisation[18]. Précisons que les données recueillies sur l'objet connecté ont fait l'objet d'un traitement avec des données statistiques pour établir une expertise sur l'état de santé de la cliente. Enfin, notons que la loi[19] « renforçant la sécurité intérieure et la lutte contre le terrorisme » en France renforce la collecte de preuves numériques, notamment à l'aide d'algorithmes permettant de recueillir automatiquement des données techniques auprès des opérateurs numériques.

---

[12] https://www.legifrance.gouv.fr/eli/ordonnance/2016/2/10/JUSC1522466R/jo/texte

[13] https://www.usine-digitale.fr/article/la-fiabilite-des-copies-numeriques-enfin-precisee.N475329

[14] http://mnbenchbar.com/2017/07/digital-evidence/

[15] Règlement (UE) n ° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (rappelons qu'un règlement s'impose à tous au sein de l'Union européenne sans nécessiter de transposition dans le droit national des États membres) : http://eur-lex.europa.eu/legal-content/FR/ALL/?uri=celex%3A32014R0910

[16] https://www.riskinsight-wavestone.com/2016/10/eidas-route-vers-europe-de-confiance-numerique/

[17] http://www.lassuranceenmouvement.com/2016/09/02/le-numerique-reduit-la-fraude-a-lassurance/

[18] https://tempsreel.nouvelobs.com/rue89/rue89-connexions-dangereuses/20141120.RUE6702/les-objets-connectes-nouvelle-boite-noire-enrolee-par-la-justice.html

[19] Loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme : https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000035932811

A travers ces exemples, on peut observer que l'admission croissante de l'information numérique comme moyen de preuve entraîne une automatisation de la collecte et du traitement d'informations ayant valeur de preuve.

Les mesures techniques pour garantir l'intégrité de la preuve numérique

Pour que l'information numérique constitue une preuve, il faut pouvoir démontrer son intégrité d'un point de vue technique. A ce titre, il ne suffit pas d'assurer la conservation du document numérique, il faut pouvoir aussi garantir sa traçabilité afin de prouver son authenticité[20]. S'il existe plusieurs outils qui permettent de gérer l'information numérique, ils ne garantissent cependant pas tous sa traçabilité et donc sa valeur probatoire.

Le choix d'un outil assurant la valeur probatoire de l'information numérique

On peut distinguer trois types d'outils différents de gestion de l'information numérique[21] :

- La gestion électronique de documents (GED) : ce type d'outil permet d'optimiser la gestion des informations numériques et leur exploitation (classement, archivage, indexation, diffusion, modification, suppression, etc.) mais ne permet pas d'assurer leur authenticité. La GED n'est pas une solution garantissant la valeur probatoire d'une information numérique ;
- Le système d'archivage électronique (SAE) : ce système intègre les règles de *records management*[22] (gestion documentaire) définies par l'organisation pour ses besoins et a pour fonction d'assurer le respect des prescriptions légales et réglementaires sur la conservation et l'intégrité des documents électroniques[23]. En outre, il doit être en mesure de garantir l'authenticité du document numérique. Ce système garantit la valeur probatoire de l'information numérique ;
- Le coffre-fort électronique : destiné à protéger les documents numériques, il permet de contrôler les accès à une information numérique et ainsi de garantir son intégrité. Néanmoins, le coffre-fort numérique reste un élément complémentaire au SAE pour garantir l'intégrité de l'information. Il n'assure pas à lui seul la valeur probatoire de l'information numérique.

Si le système d'archivage électronique constitue la solution la plus adaptée pour garantir techniquement la valeur probatoire de l'information numérique (authenticité et intégrité)[24], il est généralement nécessaire de faire appel à un prestataire spécialisé dans les services de signature électronique et d'archivage de documents numériques. A ce titre, il est nécessaire tenir compte de plusieurs critères dans le choix d'un SAE[25] :

- La conformité avec les normes de certification (NF Z 42-013 pour la France et ISO 14641-1 pour l'international) ;

---

[20] http://www.novarchive.fr/actualites/2017/04/05/avis-dexpert-tracabilite-de-linformation/

[21] http://www.novarchive.fr/faq/2015/11/03/quelles-differences-entre-ged-sae-et-coffre-fort-electronique/

[22] Méthode de gestion des documents d'archives qui consiste à contrôler de manière systématique la création, la réception, la maintenance, l'utilisation et la mise à disposition des documents numériques dans un objectif de traçabilité, d'intégrité, de sécurité et de pérennité et dans le respect des exigences légales.

[23] http://www.novarchive.fr/faq/2015/07/17/quest-ce-quun-sae-2/

[24] http://www.journaldunet.com/solutions/expert/67700/l-archivage-electronique--etape-indispensable-de-la-transformation-numerique.shtml

[25] http://www.archimag.com/demat-cloud/2017/03/21/dematerialisation-archivage-preuve-sae

- La localisation des informations numériques et la nationalité du prestataire d'archivage ;
- Les engagements des prestataires sur la mise en œuvre du SAE et sur les documents qui leur sont confiés ;
- La conformité avec les normes relatives à la sécurité des systèmes d'information telles que la famille de normes ISO/IEC 27000 ;
- La possibilité d'extraire du SAE l'ensemble des documents numériques et les éléments de preuve de leur intégrité (empreintes, journaux…) pendant toute la durée du stockage dans le SAE.

Notons que le recours à un SAE, qui centralise l'ensemble des documents numériques, peut présenter un risque. Une attaque informatique ou une panne informatique pourraient empêcher l'accès aux documents ou les endommager et ainsi remettre en cause leur valeur probatoire. En outre, la mise en œuvre d'un SAE peut être coûteuse, ce qui peut avoir pour effet de dissuader une organisation dans ses démarches de numérisation.

L'utilisation de la blockchain en matière de preuve

Afin d'améliorer techniquement la valeur probatoire de l'information numérique et de fournir une alternative aux prestataires de signature électronique et d'archivage, une nouvelle solution se développe autour de la *Blockchain*. Cette technologie permet de stocker de manière décentralisée et sécurisée les informations numériques et d'établir leur traçabilité de façon à garantir parfaitement leur intégrité. Cette perspective d'utilisation de la *lockchain* est envisagée actuellement par le Ministère de la justice au Royaume-Uni dans le cadre des preuves pénales numériques[26]. Elle est également une solution envisagée pour fiabiliser le vote électronique[27]. Néanmoins, la *Blockchain* peut présenter une limite en matière de preuve[28]. En effet, si elle permet de vérifier l'intégrité du document, de l'horodater ou de créer un lien entre un signataire et le document, elle ne permet pas d'établir un lien juridique entre l'identité du signataire et sa signature. Autrement dit, le mécanisme de la *Blockchain* ne garantit pas l'authenticité de l'information numérique au même titre que les tiers de confiance. Néanmoins, ces derniers devraient prendre en considération le développement de la *Blockchain* dans leurs solutions[29].

L'information numérique trouve peu à peu les conditions juridiques et techniques lui permettant de disposer d'une véritable valeur probatoire. Ces évolutions sont favorables, et même indispensables à l'accélération de la transformation numérique.

[26] https://cryptovest.com/news/uk-ministry-of-justice-considers-using-blockchain-to-prevent-evidence-tampering/

[27] http://www.zdnet.fr/actualites/vote-electronique-la-blockchain-a-la-rescousse-39850150.htm

[28] https://www.haas-avocats.com/data/blockchain-machine-preuve/

[29] http://www.archimag.com/demat-cloud/2017/10/10/archivage-blockchain-valeur-probatoire

La **Direction Générale des Relations Internationales et de la Stratégie (DGRIS)** propose les analyses politiques et stratégiques contribuant à renforcer l'appréciation des situations et l'anticipation. Elle soutient la réflexion stratégique indépendante, en particulier celle menée par les instituts de recherche et organismes académiques français et étrangers. Elle contribue au maintien d'une expertise extérieure de qualité sur les questions internationales et de défense.

A ce titre, la **DGRIS** a confié à **CEIS** la réalisation de cet **Observatoire du Monde Cybernétique**, sous le numéro de marché 1502492543. Les opinions développées dans cette étude n'engagent que leur auteur et ne reflètent pas nécessairement la position du Ministère de la Défense.

Ministère de la Défense
Direction Générale des Relations Internationales et de la Stratégie
60 Boulevard du Général Martial Valin – CS21623 – 75 509 Paris Cedex 15

CEIS
Tour Montparnasse – 33, avenue du Maine – BP 36 – 75 755 - Paris Cedex 15
Téléphone : 01 45 55 00 20
E-mail : omc@ceis.eu