Lettre n°50-Mai 2016-disponible sur omc.ceis.eu

« Il n'y a pas de solution unique, pas de solution miracle pour stopper l'utilisation d'Internet par les terroristes. Le partenariat public-privé doit faire partie de notre réponse globale à ce défi. Les entreprises liées à l'Internet ne peuvent pas régler ce problème seules, les Etats et les ONG non plus. Nous devons travailler de manière coordonnée. » *Steven Crown, vice-président de Microsoft, lors d'une audition au Conseil de sécurité des Nations Unies sur la menace terroriste*[1].

Table des matières

[1] http://www.rfi.fr/ameriques/20160512-terrorisme-microsoft-internet-jihadisme-cooperation-public-prive

LE DATA PROTECTION OFFICER (DPO) : ACTEUR CLE DE LA PROTECTION DES DONNEES PERSONNELLES

Une législation en pleine mutation

Après 4 ans de travaux et de négociation, le Parlement européen a adopté le 14 avril 2016 un règlement général sur la protection des données personnelles (RGDP) prenant en compte le traitement grandissant des données personnelles. Il remplacera la directive du 24 octobre 1995 sur la protection des données personnelles. Applicable à partir de 2018 sur l'ensemble du territoire des Etats membres de l'Union européenne, il représente une avancée remarquable dans l'histoire de la protection européenne des données personnelles dont le DPO se veut la pierre angulaire.

Elément crucial du « paquet sur la protection des données »[2], ce nouveau règlement a pour objectif premier l'unification et le renforcement de la réglementation de la protection des données personnelles. Il s'articule autour de trois principaux axes :

- Définition et renforcement des droits des citoyens en leur permettant de mieux contrôler leurs données personnelles dans le cyberespace ;
- Clarification et simplification des procédures administratives pour les entreprises en matière de traitement des données personnelles ;
- Création de nouveaux moyens pour veiller à l'application effective de la règlementation[3].

Pour ce faire, à l'instar des nombreuses refontes prévues, le règlement va surtout contribuer à la réforme des dispositions relatives au CIL.

Le Correspondant Informatique et Libertés, un bilan positif

Le CIL (Correspondant Informatique et liberté) a été créé par la loi du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel modifiant la loi du 6 janvier 1978 dite *Informatique et Libertés*[4]. Créé à l'initiative de l'ex-Président de la CNIL, Alex Türk, l'objectif était de mettre à la disposition des responsables de traitements tant du secteur public que privé, un nouveau moyen de s'assurer efficacement de la bonne application de la loi *Informatique et Libertés* et ainsi de préserver le droit fondamental à la protection des données personnelles.

Le CIL a différentes missions :

- Tenir un registre des traitements et assurer son accessibilité ;
- Veiller en toute indépendance au respect de la loi par la diffusion d'une culture « informatique et liberté », par le conseil et la recommandation, par l'avertissement quant au traitement de données sensibles et enfin par la médiation et la coordination ;
- Elaborer des dossiers de formalités auprès de la CNIL pour les traitements non exonérés ;
- Elaborer une politique de protection des données personnelles notamment dans le règlement intérieur et les chartes informatiques ;
- Former et sensibiliser personnel sur la réglementation applicable notamment par le prisme de formation, de brochures, etc. ;

2 Composé également de la directive relative aux transferts de données à des fins policières et judiciaires.

3 L. DE LA MONNERAYE, « Le nouveau dispositif européen de protection des données numériques », Village de la Justice, 26 avril 2016.

4 Précisée par le décret d'application n°2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

- Rendre compte de son action par l'élaboration d'un bilan annuel de ses activités à la disposition du responsable des traitements.

Afin de mener à bien leurs missions, les CIL sont épaulés par la CNIL qui organise des ateliers d'information et met en place des outils pratiques tels qu'un extranet permettant l'accès à des référentiels, des modèles, des guides et des réponses-type. La CNIL assure également une permanence téléphonique pour les assister.

La désignation d'un CIL n'est pas obligatoire mais elle présente 3 principaux avantages :

- ✓ Meilleure sécurité juridique ;
- ✓ Meilleure sécurité informatique ;
- ✓ Meilleure image[5].

Les chiffres témoignent de la place prise par le CIL au fur et à mesure du temps. Le nombre de CIL est ainsi passé de 4000 en 2008 à 14 300 fin 2014 et s'élevait à 16 300 fin 2015.[6]

Le Data Protection Officer, entre harmonisation et renforcement

Après 10 ans d'existence, le CIL va bientôt laisser sa place au Data Protection Officer (DPO). Le législateur européen a créé un personnage essentiel au centre de la protection de ces données[7]. Le rôle du DPO sera de garantir la conformité de son entité avec la règlementation de protection des données personnelles en vigueur[8]. Les responsabilités du DPO seront plus vastes et plus importantes que celles du CIL.

Contrairement au CIL, sa nomination sera obligatoire pour les autorités et organismes publics, pour les opérations de traitement exigeant un suivi régulier et systématique des personnes ou dans le cas où l'activité de la structure porte sur :

- Des données sensibles ;
- Des données de localisation ;
- Des données relatives à des enfants ou à des employés dans des fichiers de grande ampleur[9].

Le texte finalement adopté en 2016 n'a pas retenu la version initiale de l'article 35 rendant impérative la désignation d'un DPO au-delà de 250 salariés. En effet, le nombre de salariés n'est pas forcément proportionnel à la quantité de traitement des données personnelles. Il n'est pas impossible que des entreprises de taille importante ne traitent pas de données personnelles, sinon très peu, et *vice versa*. Dès lors, la suppression de cette condition aura pour effet de rendre les critères de l'obligation de désignation du DPO plus justes.

---

5 CNIL, « CIL : un métier d'avenir », 13 octobre 2015.

6 Ibidem.

7 A. GOURIO et M. GILLOUARD, « Adoption du règlement européen sur la protection des données personnelles », Revue de droit bancaire et financier, n°1, janvier 2016.

8 C. NGANDO BLACK, «3 QUESTIONS En marche vers le marché unique numérique ! », La Semaine Juridique Entreprise et Affaires, n°20, 19 mai 2016.

9 K. RIAHI, « La proposition de règlement européen relatif à la protection des données à caractère personnel : vers un marché numérique unique ? », La Semaine Juridique Edition Générale, n°9-10, 29 février 2016.

L'objectif est de créer un « CIL européen ». Le CIL actuel a en effet été créé par une loi française et, même s'il existe des homologues au CIL dans les autres pays de l'Union européenne, leurs missions ne sont pas toujours analogues.

Ce DPO aura la même fonction et le même nom dans tous les Etats de l'Union européenne. Il sera régi par un texte unique : le règlement général sur la protection des données. Il pourra éventuellement être amené à échanger avec des autorités de contrôle d'autres Etats membres.

L'une des principales différences avec le CIL est que le DPO ne sera plus seulement un « conseiller » mais un véritable « garant » de la conformité de son organisme avec la réglementation relative à la protection des données personnelles en vigueur. Aussi louable que soit cette intention de raffermissement, il est regrettable que le législateur ne précise pas si cela engage la responsabilité du DPO. Face à cette imprécision, certains spécialistes soulignent que la responsabilisation du DPO n'est pas envisageable eu égard à l'impossibilité du transfert de responsabilités du responsable de traitement au DPO[10].

Il sera par ailleurs en charge de rassembler les documents attestant que les traitements effectués sont respectueux de la règlementation applicable en la matière. Il contrôlera la conformité des traitements entrepris avec la règle du *Privacy by design*. Concernant les traitements à risques, le DPO aura pour mission de réaliser obligatoirement des études d'impact dès lors que le traitement présente un risque élevé d'atteinte à la vie privée des personnes intéressées.

Actuellement, seuls les CIL des fournisseurs de services de communication électronique ont pour obligation la notification à la CNIL et aux personnes intéressées des failles de sécurité. Or le Data Protection Officer aura l'obligation, dans toute structure, de notifier les éventuelles failles de sécurité à la CNIL, et ce, dans un délai très succinct, soit au plus tard 72 heures. Si ledit délai n'est pas respecté, le DPO devra présenter une justification valable auprès de la CNIL. Parallèlement, il devra aviser les personnes dont les données personnelles sont concernées par la faille. Très avant-gardiste, la CNIL a déjà mis en ligne le formulaire de notification de faille de sécurité.

Les avantages du DPO pour l'autorité ou l'entreprise sont multiples :

- Conseil et administration du traitement pour le compte du responsable ;
- Allègements procéduraux ;
- Interlocuteur de proximité compétent permettant un accès facilité à une information juridique adaptée à leurs activités ;
- Diffusion de culture de la protection de la vie privée au sein de l'entreprise ou de l'autorité ;
- Favorisation du *Privacy by design* ;
- Autorégulation de l'entité[11].

Actuellement, comme prévu dans le décret du 20 octobre 2005, le CIL travaille auprès du responsable de traitement mais il reste indépendant puisqu'il ne reçoit aucun ordre pour l'exercice de ses fonctions. Désormais, le règlement prévoit que le DPO sera placé auprès de la direction générale afin de le rendre encore plus indépendant, et surtout, de montrer qu'il a une place capitale. Il supprime également le seuil

10 G. PERONNE et E. DAOUD, « L'évolution du rôle du CIL à la lumière du nouveau règlement européen sur les données personnelles », Dalloz IP/IT, 2016, p. 192.

11 G. CHASSANG, « E-santé, droit de l'union européenne et protection de la vie privée des personnes : vers l'émergence d'un « technodroit » spécifique au travers de la proposition de règlement général sur la protection des données personnelles », Revue Lamy Droit de l'Immatériel, n°108, 2014.

pour désigner un CIL externe à l'entreprise. L'extériorité à l'autorité ou l'entreprise est naturellement un facteur renforçant l'indépendance du DPO.

Par ailleurs, le DPO aura des compétences supérieures à celles du CIL. En effet, si la loi du 6 janvier 1978 dispose que le CIL doit seulement bénéficier des qualifications adéquates avec cette fonction, le règlement européen va plus loin en prévoyant que le DPO doit être un véritable expert en la matière et qu'il sera sélectionné à l'aune de ses qualités professionnelles, de son expertise en la matière et de sa capacité à assumer les nouvelles fonctions prévues par le même règlement.

Cette fermeté du législateur européen au sujet de l'expertise du futur DPO s'explique par la complexité de la règlementation relative au traitement des données personnelles, qui prévoit la possibilité de demander des autorisations à des autorités de contrôle d'autres pays membres de l'Union européenne. Une bonne connaissance des procédures devant l'ensemble de ces autorités s'impose donc à l'égard du DPO.

L'année 2018 n'étant pas si éloignée, il est fortement recommandé aux autorités et aux entreprises visées par cette nouvelle disposition d'anticiper la future mise en place de Data Protection Officer. La désignation du DPO ne sera pas chose facile compte tenu des responsabilités qui pèseront sur ses épaules et des enjeux, qu'il s'agisse de l'ampleur des sanctions encourues (20 millions d'euros ou 4% du chiffre d'affaires annuel mondial pour les entreprises), du risque d'image, et, dans l'hypothèse d'une fuite de données, de l'indemnisation des personnes dont les données personnelles auront été divulguées.

Bien que leurs responsabilités soient étendues, les CIL actuels deviendront très certainement les futurs DPO, et à ce titre, il faut que les CIL commencent à anticiper les adaptations à réaliser au sein de l'entreprise. Le rôle du DPO sera de garantir la conformité de sa structure à l'aide du principe d'*accountability* par la mise en place par exemple de *binding corporaterules* (règles internes à l'entreprise) permettant de contrôler le traitement et le transfert tant intracommunautaire qu'extracommunautaire des données à caractère personnel. Ce nouvel acteur devra par ailleurs travailler en coordination avec d'autres services dont le responsable des traitements, les sous-traitants ou encore le RSSI.

La substitution du CIL en DPO nécessitera incontestablement un grand travail de formation. La CNIL aura donc une mission cruciale dans la formation de ces futurs DPO. Par ailleurs, il pourrait être envisagé de futures formations universitaires spéciales « Data Protection Officer » à l'image des actuels Master 2« Compliance Officer »[12]. L'analyse de l'importance des nouvelles missions et du renforcement des missions antérieures du DPO conduit à un constat immédiat : les difficultés de conciliation entre la profession quotidienne du DPO et ses missions de DPO. Les entités visées devront a priori créer un poste nouveau à plein temps pour le DPO ou alors faire appel à un DPO extérieur[13].

Conclusion

Loin d'être une évolution purement sémantique, la transformation du CIL en DPO apporte de nouveaux éléments et s'inscrit parfaitement dans la transformation numérique de la société. Au cœur de la protection des données personnelles de l'*Homo numericus,* le DPO incarnera progressivement une figure

12 Comme le Master 2 Juriste sécurité financière / Compliance officer sous la direction de Madame C. CUTAJAR de l'Université de Strasbourg.

13 G. PERONNE et E. DAOUD, opt. cit.

indispensable[14]. Anticipant l'entrée en application du règlement, le vocable de « Data Protection Officer » s'est d'ailleurs déjà imposé[15] au détriment de celui de Délégué de la Protection des Données.

14 H. LEGRAS, « 3 Questions La métamorphose du CIL en DPO », La Semaine Juridique Entreprise et Affaires, n°7, 12 février 2015.

15 G. PERONNE et E. DAOUD, opt. cit.

LES APPLICATIONS DE LA TECHNOLOGIE *BLOCKCHAIN*

Annoncée comme la prochaine révolution, la Blockchain est une technologie de stockage et de transmission d'information, transparente et sécurisée. Il s'agit littéralement d'une chaîne de blocs numériques au sein desquels peuvent être stockées des informations de toutes natures, constituant une base de données partagée par tous ses utilisateurs.

Son architecture, mêlant cryptographie et réseau de type distribué, rend infalsifiable l'information qu'elle contient : il faudrait pour ce faire avoir le contrôle de plus de la moitié de l'infrastructure globale. Fonctionnant sans organe de contrôle, elle fait ainsi reposer la confiance en l'information sur l'algorithme lui-même, ouvrant la voie à des projets inédits. En effet, si la technologie Blockchain est apparue avec la crypto monnaie Bitcoin, son architecture intéresse aujourd'hui de nombreux acteurs (entreprises, gouvernements, etc.) pour d'autres applications. On peut regrouper celles-ci en trois catégories :

- Le transfert d'actifs ;
- La tenue de registre ;
- Les *Smart Contracts*.

Le transfert d'actifs

Une économie de 15 à 20 milliards de dollars par an pour le secteur bancaire à l'horizon 2022 grâce à la Blockchain : telle est la prévision de la banque Santander dans son rapport publié en 2015. Cette économie est réalisable grâce à une importante baisse des coûts de structure liée à l'activité des paiements internationaux. La Blockchain permet en effet le transfert d'une valeur monétaire entre deux entités sans avoir recours à un tiers de confiance, diminuant ainsi le coût lié à cette transaction. Si traditionnellement, le transfert de monnaie se fait par le biais d'un intermédiaire rémunéré par lequel transite ce flux monétaire, la Blockchain permet de s'en affranchir et d'aboutir au même résultat de manière plus sécurisée et moins coûteuse. Les transferts de Bitcoin par exemple ne prennent théoriquement que quelques minutes (normalement 10 minutes au maximum, ce qui équivaut au temps nécessaire à la validation du bloc et de son intégration à la chaîne Bitcoin).

Les propriétés intrinsèques de cette technologie ouvrent le champ à de nouvelles perspectives concernant le marché du transfert de devises. C'est l'exemple de la startup française Moneytis[16], dont le business model repose en partie sur la technologie Blockchain. Le service proposé par la startup est le transfert d'argent sans le recours à un intermédiaire, avec un coût 9 fois inférieur à celui pratiqué par les établissements traditionnels. Voyant venir le danger, BNP Paribas se positionne déjà sur le « marché » de la Blockchain en nouant un partenariat avec la plateforme de financement participatif SmartAngels[17]. A travers ce partenariat, la banque souhaite utiliser la technologie Blockchain comme un relais de croissance vers d'autres marchés, en proposant de nouvelles formes de financement participatif destiné aux PME.

Le souhait de BNP Paribas d'investir dans ce secteur répond à deux objectifs stratégiques. Le premier est l'appropriation et l'intégration de cette innovation qui est susceptible de devenir une menace de plus en plus sérieuse pour l'ensemble des acteurs financiers (risque de la disparition des barrières à l'entrée). Le second

16 https://moneytis.com/

17 http://www.challenges.fr/challenges-soir/20160405.CHA7335/bnp-paribas-joue-les-pionniers-dans-le-Blockchain.html

est de bénéficier du caractère décentralisé, ultra sécurisé et surtout inviolable de la Blockchain pour sécuriser les transactions financières et valider les contrats.

De ce fait, la Blockchain permet non seulement la mise en relation entre détenteurs et demandeurs de capitaux, mais aussi la tenue d'un registre permettant de stocker l'ensemble des opérations de manière sécurisée et transparente.

La tenue de registre

Les Blockchains sont des « livres de comptes » qui enregistrent de façon immuable l'ensemble des informations traitées et validées d'un service donné. Ces informations, de natures diverses, sont réputées infalsifiables. Le virement d'une crypto monnaie par exemple entraîne systématiquement l'enregistrement de l'ensemble des informations relatives aux utilisateurs et aux transactions. Cette propriété permet une grande transparence dans les échanges entre les utilisateurs car l'ensemble des transactions est partagé et enregistré par le réseau.

La disponibilité du code source de la technologie Blockchain a permis le développement de nouveaux types de Blockchains adaptées aux besoins des entreprises et des gouvernements. Le Honduras a par exemple adopté un registre de titres fonciers basé sur la Blockchain. L'enjeu pour le pays est de développer un registre infalsifiable qui comporte l'ensemble des informations de propriété des citoyens. Ce projet, mis en place par le gouvernement du pays avec l'entreprise américaine Factom Inc., a pour objectif de lutter contre les fraudes (notamment la modification de bases de données par des fonctionnaires corrompus[18]) liées aux titres de propriété.

Les *Smart Contracts*

L'architecture de la technologie Blockchain a également inspiré un jeune développeur canadien de 22 ans, Vitalik Buterin, et l'a conduit à créer la Blockchain Ethereum. Celle-ci, qui dispose de sa propre crypto monnaie appelée Ether, repose sur un protocole permettant la création de contrats intelligents, ou *Smart Contracts*. Ces contrats permettent d'associer un transfert automatisé de valeur à la réalisation de conditions mutuellement convenues à l'avance.

Les *Smart Contracts* sont des applications destinées à répondre à un besoin de sécurité, de confiance et de transparence. La différence entre ces derniers et les contrats classiques réside dans le fait de pouvoir faire confiance au « code informatique » en lieu et place d'un tiers de confiance traditionnel. En effet, les *Smart Contracts* peuvent être définis comme un programme informatique qui exécute des tâches après la vérification de conditions préalablement définies.

Contrairement à la Blockchain Bitcoin, dédiée uniquement aux transactions financières, le champ d'application des *Smart Contracts* qu'apporte l'Ethereum est très large et concerne plusieurs secteurs d'activité. De la finance à la location de bien immobilier ou le notariat, les *Smart Contracts* sont susceptibles de bouleverser plusieurs secteurs d'activité et métiers.

C'est notamment le cas du secteur de l'assurance, comme en témoigne l'investissement de plus de 55 millions[19] de dollars de l'entité Axa Strategic Ventures dans la startup canadienne Blockstream. Le protocole

18 http://innovation.talan.fr/fr/2016/02/09/un-titre-de-propriete-inscrit-sur-la-Blockchain-a-t-il-une-valeur-legale/

19 https://www.axa.com/fr/newsroom/actualites/axa-strategic-ventures-Blockchain

développé par cette dernière, Sidechain, est actuellement l'un des plus aboutis du marché en termes de sécurité. Il permet de faire interagir des réseaux privés et publics entre eux afin d'assurer une sécurité maximale des transactions.

A titre d'exemple, les *Smart Contracts* redéfiniront le business model du secteur de l'assurance sur deux points essentiels :

- L'allègement considérable, tant pour les assurés que pour les assureurs, des démarches de déclaration, de validation, de vérification et de déclenchement du paiement. Autrement dit, cela permettra à l'assureur de diminuer les coûts de structure inhérents à la réalisation de ces tâches via l'automatisation du processus. Un agriculteur pourra par exemple théoriquement s'assurer contre le risque de sécheresse par le biais d'un Smart Contract. L'application Blockchain hébergeant le Smart Contract collectera automatiquement les données pluviométriques de la région concernée et exécutera automatiquement le contrat selon les conditions prédéfinies.
- Le développement des *Smart Contracts* permettra la mise en place d'entités totalement autonomes, où l'exécution des termes du contrat d'assurance pourra être validée et vérifiée par l'ensemble des acteurs du réseau P2P. De ce fait, la Blockchain se positionne comme étant le tiers de confiance.

Dans le domaine de l'énergie, les *Smart Contracts* peuvent également jouer un rôle majeur en proposant de nouvelles applications décentralisées. C'est le cas de la coopérative TransActiveGrid[20] qui a créé un réseau d'électricité basé sur la technologie Blockchain. Il s'agit d'une application qui permet d'échanger de l'énergie solaire de façon décentralisée entre des particuliers, eux-mêmes producteurs d'énergie solaire, en fonction de leurs besoins. Cette nouvelle forme de consommation pourrait permettre une baisse considérable des coupures d'électricité dans certains pays et une réduction des coûts pour le consommateur final.

La signature électronique est aussi investie par la technologie Blockchain. Ainsi, la startup française BlockSign propose un service Blockchain de signature électronique de documents permettant de signer, faire signer et vérifier l'authenticité d'un document, ainsi que d'émettre des factures réglables en Bitcoin.

Autre domaine susceptible d'intégrer la technologie Blockchain : le vote en ligne. Partant du constat fait par l'institut américain Brennan Center For Justice américain que la plupart des machines à voter des Etats-Unis auront dix ans d'existence[21] en novembre 2016 et que ces machines obsolètes étaient vulnérables, la bourse technologique de New York[22] a annoncé que les votes en ligne des actionnaires s'effectueraient désormais grâce la technologie Blockchain. Pour le Nasdaq, qui dispose d'ores et déjà de son propre système de Blockchain Linq[23] pour le stockage et l'authentification des documents, l'adoption du vote en ligne permettra ainsi l'enregistrement rapide des votes en toute sécurité.

Conclusion

L'engouement autour de la technologie Blockchain s'inscrit dans une tendance globale de désintermédiation qu'engendre la dématérialisation croissante des services. Loin de se cantonner à la monnaie virtuelle, les applications de la Blockchain se développent dans de nombreux secteurs (banque, assurance, notariat,

20 https://rslnmag.fr/cite/la-Blockchain-le-futur-des-reseaux-delectricite-2

21 https://www.brennancenter.org/publication/americas-voting-machines-risk

22 http://www.lemondeinformatique.fr/actualites/lire-le-nasdaq-va-utiliser-un-Blockchain-pour-enregistrer-les-votes-des-actionnaires-63922.html

23 http://www.lemondeinformatique.fr/actualites/lire-le-nasdaq-va-utiliser-un-Blockchain-pour-enregistrer-les-votes-des-actionnaires-63922.html

etc.), à tel point que certains acteurs numériques traditionnels tels qu'IBM ou Microsoft se lancent dans le Blockchain-as-a-Service (BaaS). Objectif : proposer un environnement de développement permettant de créer facilement une application Blockchain adaptée aux besoins de l'entreprise.

La raison de cet engouement, tant dans les secteurs public que privé, tient au fait que la Blockchain permet de créer des modèles organisationnels de confiance fonctionnant en toute autonomie, de manière sécurisée et à moindre coût. Pourtant, l'indépendance qu'elle procure n'est pas accueillie positivement par l'ensemble des acteurs, notamment étatiques. La Russie a récemment présenté un projet de loi[24], qui sera voté en juin, visant à interdire l'utilisation du Bitcoin. Le ministère des Finances estime que *«l'utilisation de ces monnaies crée les conditions préalables à la participation des citoyens et des personnes morales à des activités illégales, y compris de blanchiment d'argent »*.

Dans la pratique, le combat se révèle difficile. Malgré les mesures restrictives du gouvernement visant à décourager l'utilisation des crypto monnaies depuis quelques années, les deux principales plateformes d'échange de la monnaie virtuelle en Chine, OKCoin et Huobi, représentent désormais à elles seules plus de 90% des échanges mondiaux de bitcoins[25]. Le 30 mai 2016 voyait encore des achats massifs de Bitcoin par des utilisateurs chinois : 1,6 million de bitcoins ont été achetés en l'espace d'une journée, un mouvement qui semble notamment motivé par la déflation du Yuan par rapport au dollar.

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 et des Anciens combattants
Direction Générale des Relations Internationales et de la Stratégie
14 rue Saint-Dominique - 75700 – Paris SP 07

CEIS
280 Boulevard Saint-Germain - 75007 - Paris
Téléphone : 01 45 55 00 20
E-mail : omc@ceis-strat.com

24 http://www.mag-securs.com/news/articletype/articleview/articleid/34792/bitcoin-les-utilisateurs-russes-risquent-gros-desormais.aspx

25 http://bfmbusiness.bfmtv.com/bourse/quand-les-investisseurs-chinois-font-flamber-le-bitcoin-978965.html