Le Mag

Confiance numérique : valeur, risques et opportunités

#2
OCTOBRE 2022

CNCC
COMPAGNIE NATIONALE DES COMMISSAIRES AUX COMPTES

édito

Alors que la majeure partie de l'activité économique repose aujourd'hui sur les systèmes d'information et les infrastructures numériques, la notion de « confiance numérique » doit être au cœur des préoccupations des dirigeants. Il s'agit d'un un enjeu de valeur, de pérennité et, in fine, de croissance. La confiance est le meilleur carburant de la croissance. Cette affirmation est tout aussi valable pour la confiance numérique, facteur essentiel au bon fonctionnement de toutes les organisations – entreprises, associations, institutions, etc. – et de l'économie en général.

Pour gagner cette confiance, les dirigeants doivent se poser les bonnes questions en termes de technologies, de risques, de maîtrise des données, et être irréprochables dans leur communication à destination de leur environnement sur ces questions. Les accompagner sur ce terrain fait aussi partie de la mission des commissaires aux comptes, profession créatrice des conditions de confiance et de sécurité de la sphère économique, sociale et environnementale.

En matière de confiance numérique, nous avons une légitimité indéniable, non pas en tant qu'experts techniques des systèmes d'information – nous n'y avons jamais prétendu ! – mais en tant qu'alliés des dirigeants dans l'identification des risques qui pèsent sur la pérennité de leur organisation et en tant que garant de leur capital confiance vis-à-vis de leurs parties prenantes.

Nos pratiques professionnelles et nos missions évoluent, au diapason des innovations technologiques et du cadre législatif, pour nous permettre de remplir pleinement notre mission d'intérêt général auprès des entités auditées, y compris sur ce volet. C'est notre rôle, en tant qu'institution, d'anticiper et d'accompagner ces évolutions.

Bonne lecture !

Yannick Ollivier

Président de la CNCC

sommaire

PHOTOS : COUVERTURE : © UNSPLASH - P2-3 : CNCC - DR - © PXHERE

CB NEWS

CNCC COMPAGNIE NATIONALE DES COMMISSAIRES AUX COMPTES

#2 OCTOBRE 2022

Responsable éditorial
Tanguy Leclerc

Coordination Annonceur
Hélène Aubinais

Crédits Photos
Unsplash /© Michal Kubalczyk

Maquette
Graphic Linked

Impression
Imprimerie Compédit Beauregard

Événement

NUMÉRIQUE : AU-DELÀ DE LA TRANSFORMATION, UN ENJEU DE CONFIANCE

Quel que soit leur niveau de maturité face au défi de l'adaptation numérique permanente, toutes les organisations sont confrontées à travers elle à de nouveaux enjeux de confiance. Les prendre en compte n'est plus une option.

À l'ère du digital, les systèmes d'information et les infrastructures numériques constituent un enjeu stratégique majeur pour les organisations, devenant un de leurs principaux leviers de croissance et de performance. Suivant les évolutions technologiques, la transition numérique s'accélère et questionne la nature même de l'entreprise, sa valeur – notamment celle de ses actifs immatériels et en premier lieu ses datas – et la manière dont elle produit cette valeur. Si l'essor de la digitalisation des processus ouvre des opportunités de croissance et d'innovation inédites, il s'accompagne également de nouveaux dangers : violation de données, rançongiciels, risque réputationnel, non-conformité au règlement sur la protection des données, etc. Ces risques pèsent sur l'entreprise, mais pas seulement. Ils pèsent aussi sur ses parties prenantes, faisant émerger un besoin accru de confiance, dont les conditions sont multiples : maîtrise des technologies (blockchain, automatisation des processus robotisés, intelligence artificielle, etc.), des risques cyber, de l'exploitation des données, etc. Les organisations ou les entreprises sont en position de devoir fournir toujours plus d'assurances à leur environnement quant à la transparence et à la qualité de l'information qu'elles communiquent ces sujets.

LES COMMISSAIRES AUX COMPTES, ACTEURS DE LA CHAÎNE DE CONFIANCE NUMÉRIQUE

Cette nouvelle exigence, à attacher à la notion de « confiance numérique », était au cœur de la journée d'échanges organisée par la CNCC le 22 mars dernier sur le campus Station F, à Paris. Un événement qui fut l'occasion de dresser un état des

Une entreprise, aussi performante soit-elle, peut être mise à terre ou décrédibilisée si elle protège mal ses données et celles de ses clients.

lieux sur la maturité des entreprises françaises face aux enjeux économiques et réglementaires liés à la confiance numérique, et d'insister sur le rôle des auditeurs pour sensibiliser les entreprises et prendre une part active au maintien du niveau de transparence et de sécurité numérique nécessaire aux échanges et à la croissance.

Yannick Ollivier, Président de la CNCC, y a défendu l'idée qu'au-delà d'être un enjeu de valeur, la confiance numérique est aussi un enjeu de pérennité, c'est-à-dire de sécurisation de la valeur : « une entreprise, aussi performante soit-elle, peut être mise à terre ou décrédibilisée si elle protège mal ses données et celles de ses clients ».

L'adage « mieux vaut prévenir que guérir » s'applique tout particulièrement à la cybersécurité. Les chiffres rendus publics par l'Agence Nationale de la Sécurité des Systèmes d'Information (l'ANSSI) témoignent de la montée en puissance des cyber-attaques commises à l'encontre des entreprises ou des organismes institutionnels depuis la crise du COVID : en 2021, 2089 signalements ont été recensés, dont 8 incidents majeurs, 203 attaques par rançongiciel et 17 opérations de cyberdéfense ont été déployées en réponse. De son côté, la CNIL a reçu 5 037 notifications de violations de données, en hausse de 79% par rapport à 2020.

Une certitude : tout le monde est susceptible d'être touché, que ce soit à titre individuel ou professionnel. Face à cette menace, les dirigeants d'entreprise n'ont pas d'autres choix que de s'interroger sur la bonne maîtrise des technologies qu'ils choisissent et sur la manière dont ils les utilisent, leur exposition au risque cyber et la manière dont ils préviennent ce risque, les données qu'ils recueillent et qu'ils exploitent.

Pour ce faire, les entreprises peuvent compter sur ...

PHOTO : DR

L'idée n'est pas de transformer les commissaires aux comptes en délégués à la protection des données, mais d'en faire les acteurs de la sensibilisation, pour le respect du RGPD notamment.

Ci-dessus, de gauche à droite : **Rémy Ozcan** (FFPB), **Hugo Bordet** (ADAN), **Fabrice Heuvrard** (expert-comptable)

l'expertise des commissaires aux comptes, alliés du dirigeant dans l'identification et la prévention des risques. « Nous devons communiquer auprès de l'écosystème business pour faire valoir leur place de tiers de confiance sur le terrain du numérique », commente Yannick Ollivier.

NOUVEL ENJEU DE CONFIANCE, NOUVELLES PRATIQUES POUR LES AUDITEURS

« L'idée n'est pas de transformer les commissaires aux comptes en délégué à la protection des données (DPO) mais d'en faire les acteurs de la sensibilisation pour le respect du RGPD notamment, en faisant un focus sur un point essentiel qui est la bonne connaissance du système d'information par la gouvernance de l'entreprise, explique pour sa part Arnaud Ducap, Vice-Président de la commission Prospective & Innovations de la CNCC. Nous sommes à la croisée de chemins sur la manière dont les nouvelles technologies comme la blockchain, l'intelligence artificielle et le RPA (Robotic Process Automation, NDLR) vont impacter nos métiers au quotidien. » Et de s'appuyer sur l'exemple des directeurs financiers en entreprise qui, par la force des choses, deviennent des Chief Value Officer (CVO), responsables de la sécurisation de la valeur de l'entreprise. « Leurs équipes ne passeront plus que 10 à 20 % de leur temps à produire l'information et la vérifier comptablement parlant, contre 50% auparavant. Notre objectif premier en tant que commissaires aux comptes est de comprendre comment cette information et ces données sont produites et quel est le cycle de collecte et de traitement de cette information chez nos clients. » À ce titre, l'IA est un atout précieux pour faciliter un audit de confiance. Elle permet entre autres d'automatiser les tâches manuelles ; d'identifier les anomalies (paiements inhabituels et transactions à risque) ; d'analyser la totalité des données structurées et non structurées ; et de prévoir les futurs risques et événements grâce à l'analyse des données historiques de paiement.
Les commissaires aux comptes évoluent dans un environnement où l'exercice de leur jugement aura de plus en plus de valeur. « Nous sommes encore à l'aube d'une grande aventure, qui inscrit en profondeur et de manière pérenne les commissaires aux comptes au cœur des enjeux numériques », conclut Yannick Ollivier. ●

PHOTO : DR

INFOGRAPHIE

Les dirigeants des PME-ETI face aux risques cyber

95%

des dirigeants de PME-ETI déclarent avoir l'impression de bien connaître ce qu'est la cybersécurité.

25%

d'entre eux seulement estiment que leur entreprise présente un risque élevé d'être touchée par une attaque.

Source : Étude Xefi/Ifop publiée le 13 décembre 2021

58%

des sondés estiment qu'ils font face à un niveau de risque équivalent à celui de l'an dernier.

29%

estiment que le risque augmente par rapport à l'ère pré-covid.

88%

sont confiants dans leur capacité à gérer une cyber-attaque si elle survenait.

41%

des dirigeants estiment mieux maîtriser leurs risques.

26%

seulement pensent pouvoir les gérer totalement, les autres estimant devoir être accompagnés par des professionnels.

Gestion des risques

Elle devient de plus en plus prégnante pour les PME et ETI et est perçue comme l'un des éléments sur lesquels repose le plus leur compétitivité :

1. Stratégie commerciale — 61%
2. Innovation et R&D — 52%
3. Gestion des risques — 51%

Moyens mis en place

46% des PME et ETI ont déployé des moyens de protection supplémentaires face aux cyber-menaces au cours de l'année écoulée :

- Par la sensibilisation et la formation des collaborateurs — 85%
- Par la mise à jour de leurs logiciels — 78%

Source : Baromètre QBE/OpinionWay

Focus

PROSPECTIVES ET INNOVATION : LA CNCC À LA MANŒUVRE

Soucieuse d'anticiper l'impact que pourraient avoir les technologies émergentes sur la profession et ses clients, la Compagnie s'efforce de proposer les outils à même de favoriser l'acculturation des commissaires aux comptes et d'accélérer leur formation.

Les pratiques professionnelles et les missions des commissaires aux comptes évoluent au diapason des technologies et du droit, leur permettant de remplir pleinement leur mission d'intérêt général auprès des entités auditées. La CNCC, et en son sein la commission Prospectives & Innovation (CPI) présidée par Nathalie Malicet, accompagne les professionnels dans ce mouvement et met à leur disposition un certain nombre d'outils et de formations qui couvre l'ensemble des nouveaux enjeux auxquels ils sont confrontés. Ces actions viennent servir la transition numérique des cabinets aussi bien que l'enrichissement et le développement de leurs prestations, au service du capital confiance de leurs clients sur le volet numérique.

Une mission d'autant plus indispensable que la majorité des PME françaises sont loin d'être suffisamment armées face aux risques cyber. « La plupart des dirigeants sont encore dans le déni, convaincus qu'ils ne sont pas une cible intéressante pour être un jour victime d'une cyberattaque », constate Nathalie Malicet. « Or, la réalité, c'est que nous avons tous été ou nous serons tous un jour ou l'autre victimes d'un acte malveillant pour la bonne et simple raison que l'immense majorité des attaques se font à l'aveugle », insiste-t-elle.

LE CYBER RISQUE EST AVANT TOUT UN PROBLÈME DE GOUVERNANCE

Dans ce contexte, le rôle de prévention des auditeurs sur les risques qui pèsent sur l'entreprise est primordial. Par leur bonne connaissance du système d'information de leurs clients les auditeurs sensibilisent la gouvernance sur la nécessité de sécuriser les maillons de la chaîne

« À nous de prendre le pouls des tendances actuelles et futures, de leur rythme d'adoption par nos clients et des enjeux que cela va représenter pour la profession en termes d'évolution des techniques d'audit. »

Nathalie Malicet, Présidente de la commission Prospectives & Innovation (CPI)

Ci-dessus, de gauche à droite : **Arnaud Ducap** (Vice-président de la CPI), **Nicolas Catel** (membre de la CPI) et **Nathalie Malicet** (Présidente de la CPI)

de collecte et d'exploitation des données. « L'erreur classique est de considérer qu'il s'agit d'une problématique IT, or le cyber-risque est avant tout un problème de gouvernance », insiste Nathalie Malicet.

La première mission de la CPI est, comme le rappelle sa présidente, de favoriser l'acculturation pour des commissaires aux comptes qui ne s'estiment pas suffisamment concernés ou pas suffisamment au point techniquement parlant.

« Il s'agit de leur démontrer qu'il existe aujourd'hui des outils d'utilisation simples, qui permettent d'aborder ces missions d'audit avec plus de sécurité et de confort et donc plus de rentabilité, dès lors qu'on les maîtrise correctement », explique Nathalie Malicet. Ainsi en est-il de RGPD Audit, un outil développé depuis un an sur le même modèle que la plateforme CyberAUDIT, qui permet de réaliser un diagnostic sur la démarche de mise en conformité de l'entreprise puis de simuler des scénarii de violation de données et d'évaluer leur coût financier. Cet outil est complété, pour les professionnels, par un guide RGPD, édité début mars et téléchargeable depuis le site de la CNCC. La CPI a d'autre part mis sur pieds avec CNCC Formation un programme ambitieux sur les sujets systèmes d'information, cybersécurité, numérique et protection des données *(voir page suivante)*.

La troisième mission que se fixe la CPI est d'assurer, via un groupe de travail dédié, une veille

...

PHOTOS : DR

CNCC FORMATIONS **CYBER / NUMÉRIQUE**

LA CNCC INVESTIT, POUR UNE PROFESSION EN POINTE SUR LES ENJEUX NUMÉRIQUES

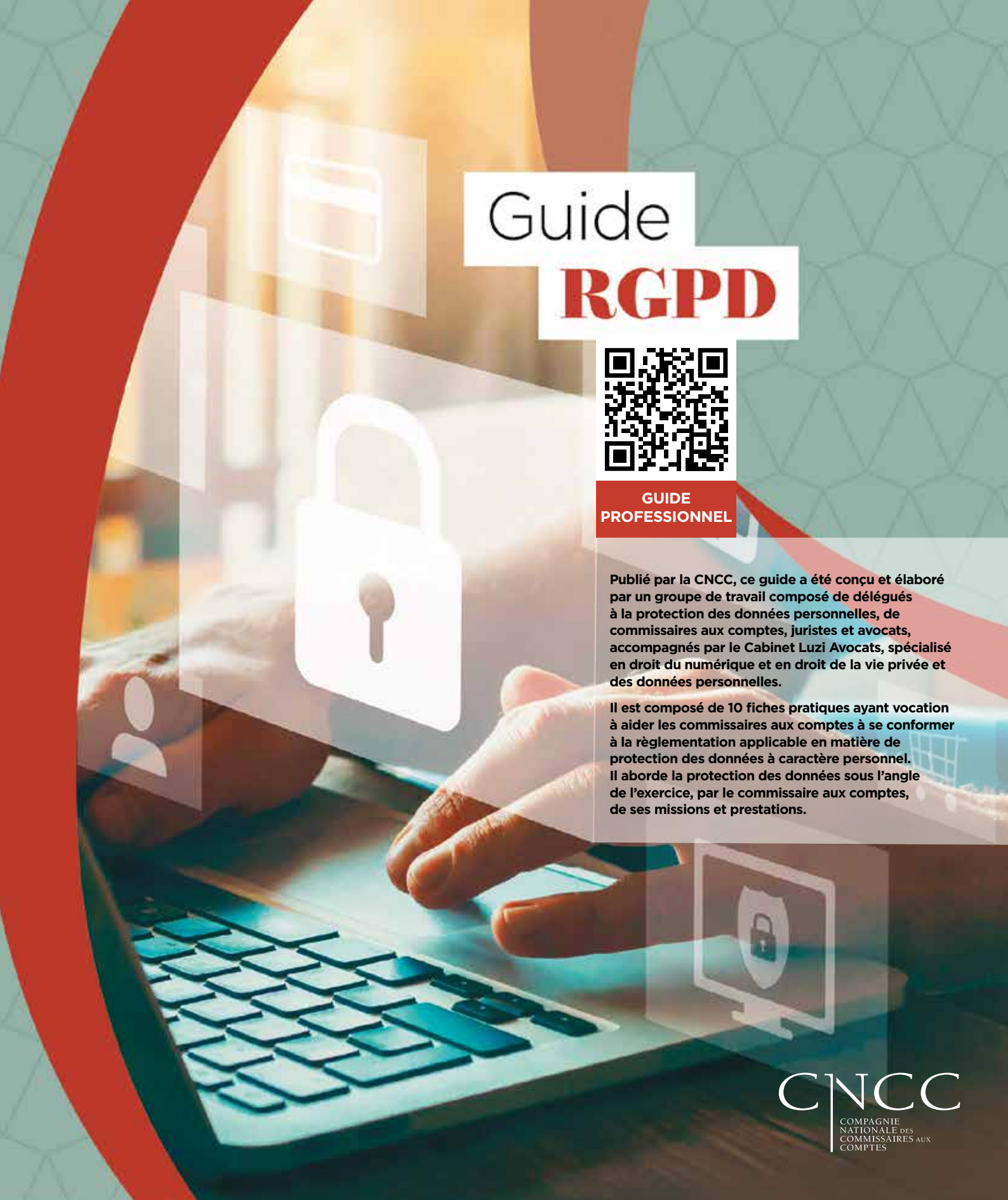
- **Blockchain : évolution ou révolution du métier d'auditeur ?**
- **Découvrir et auditer les actifs numériques.**
- **Découvrir et maitriser les fondamentaux de l'informatique et de la cybersécurité.**
- **Audit des PME et transition numérique : risques et atouts.**
- **Le commissaire aux comptes, acteur de la cybersécurité.**
- **L'IA, le big data, le machine learning, quelles applications pour l'audit ?**
- **Maîtriser la cybersécurité pour apprécier les organisations des clients et accompagner les dirigeants d'entreprise.**
  Formation labellisée par l'ANSSI.
- **Réaliser un diagnostic RGPD : une nouvelle mission pour le commissaire aux comptes. Savoir utiliser l'outil RGPD AUDIT© avec efficacité.**
- **Data et programmation pour les commissaires aux comptes.**
- **Conflits internationaux : quel impact sur la cybersécurité des entreprises françaises ?**
- **L'audit des systèmes d'information dans le cadre de la certification des comptes : principes et concept.**
- **Mettre en œuvre le guide d'hygiène informatique de l'ANSSI.**
- **Auditer les systèmes d'information / Bases techniques et approches pratiques.**

Informations et inscriptions sur le site de CNCC Formation
formation.cncc.fr **#laformationnaturellementcac**

technologique sur l'impact que pourraient avoir sur la profession les technologies émergentes. « Notre présence à divers événements internationaux nous permet de pouvoir prendre le pouls des tendances actuelles et futures, de leur rythme d'adoption par nos clients et des enjeux que cela va représenter pour la profession en termes d'évolution des techniques d'audit, des nouveaux risques pour nos clients et également des réponses à leur apporter sur les enjeux de sécurité et de confidentialité » déclare Arnaud Ducap, vice-président de la CPI. « En juin 2021, notre immersion à Vivatech nous a ainsi permis de mieux identifier les enjeux de sortie de confinement Covid et d'accélération des transformations. Début 2022, notre présence au CES de Las Vegas nous a permis de poursuivre nos investigations sur les tendances identifiées lors de Vivatech, comme le développement des usages de la blockchain, de l'intelligence artificielle ou de l'automatisation, et ainsi centrer une partie des travaux de la commission sur ces enjeux pour « acclimater » la profession :

- enjeux réglementaires avec la nouvelle réglementation européenne « digital service » et le « Digital Market Act »,
- enjeux d'attractivité pour les jeunes générations,
- enjeux d'efficacité par la maitrise des technologies et identification des partenariats pour faciliter la digitalisation de la profession. »

Les travaux de la commission pour 2022 se poursuivent pour tester des solutions et des technologies identifiées, ou des environnements comme les métavers, et proposer à la fois des réponses à court terme et à moyen long / terme selon le niveau de maturité des technologies. « On peut légitimement se demander ce que viendraient faire les commissaires aux comptes dans ces univers virtuels, indique Nathalie Malicet. La réponse est aujourd'hui, rien, ou presque. Mais demain ? Quand nous aurons comme clients des entreprises qui ont choisi d'investir dans ces environnements et dans les technologies associées sous forme de placements financiers, il nous faudra savoir ce qu'est le métavers, réfléchir à ses impacts économiques et aux risques associés, pour être en mesure de jouer notre rôle auprès d'elles et au sein de l'économie. »



Guide RGPD

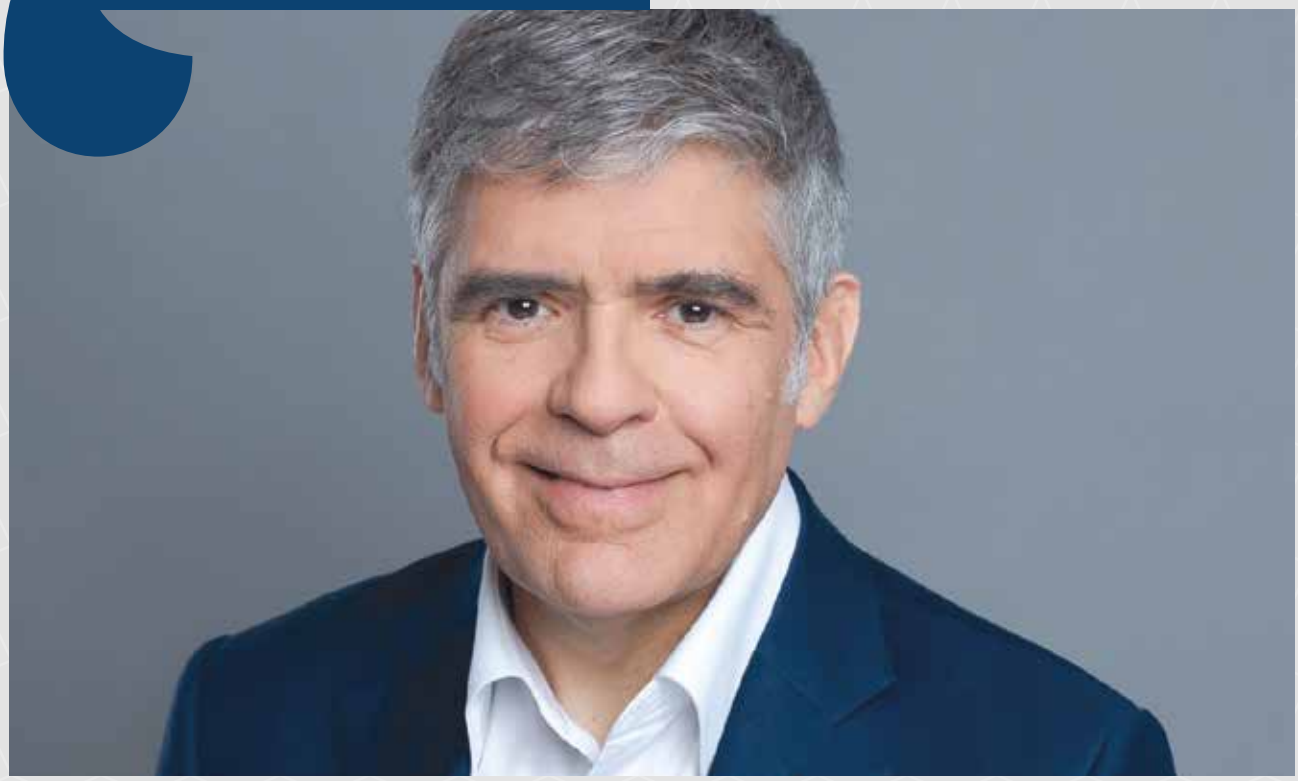
GUIDE PROFESSIONNEL

Publié par la CNCC, ce guide a été conçu et élaboré par un groupe de travail composé de délégués à la protection des données personnelles, de commissaires aux comptes, juristes et avocats, accompagnés par le Cabinet Luzi Avocats, spécialisé en droit du numérique et en droit de la vie privée et des données personnelles.

Il est composé de 10 fiches pratiques ayant vocation à aider les commissaires aux comptes à se conformer à la règlementation applicable en matière de protection des données à caractère personnel. Il aborde la protection des données sous l'angle de l'exercice, par le commissaire aux comptes, de ses missions et prestations.

CNCC
COMPAGNIE NATIONALE DES COMMISSAIRES AUX COMPTES

INTERVIEW **CHRISTIAN POYAU**



« Bien au-delà de la technique, la cybersécurité est une question de sensibilisation »

Christian Poyau

Co-président de la commission Mutations technologiques et Impacts sociétaux du Medef, PDG de Micropole.

Quel état des lieux faites-vous de la maturité des entreprises françaises face aux enjeux de la transformation numérique ?

CHRISTIAN POYAU_ Les entreprises en France sont globalement en retard sur le sujet. À l'occasion de la dernière édition de VivaTech, le MEDEF a publié avec le Boston Consulting Group (BCG) une étude portant sur la maturité digitale de la France post crise sanitaire, et les résultats mettent en évidence le fait que nos TPE et PME ont adopté un socle digital essentiel notamment en matière d'outils collaboratifs et de comportements cyber, mais qu'elles doivent passer désormais un cap pour transformer en profondeur leur activité. Si la majorité des dirigeants d'entreprises placent la flexibilité, la sécurité et la durabilité au cœur de leurs préoccupations, les PME sont encore trop peu nombreuses à se saisir du potentiel des datas pour se moderniser et gagner en compétitivité. Un quart des PME sondées dématérialisent la relation client et renforcent leur présence en ligne, mais plus de la moitié n'ont pas démarré et ne réfléchissent pas encore à la valorisation de leurs données, ce qui, dans le contexte compétitif actuel, est un vrai handicap.

PHOTOS : DR

À quoi est due cette frilosité ?

C. P._ La prise de conscience des enjeux n'a pas résolu la principale interrogation des dirigeants d'entreprise, qui est « comment je fais ? ». Cela suppose du temps, des compétences et une capacité de financement. Or la majorité des blocages se situent sur les deux derniers points. Les PME-TPE rencontrent les plus grandes difficultés à recruter les profils « digitaux » adéquats, et par ailleurs la fiscalité nationale freine sensiblement leur capacité d'investissement. Le niveau de rentabilité des entreprises françaises est inférieur de 5 à 10 points par rapport à leurs concurrents européens, ce qui n'est évidemment pas négligeable.

Comment éviter que le virage du numérique ne débouche sur un fossé entre les entreprises qui l'ont déjà pris et celles qui sont en retard ?

C. P._ Nous devons veiller à ce que ce fossé ne se creuse pas, et c'est justement l'enjeu du travail que nous menons au sein de la commission Mutations technologiques et impacts sociétaux. D'où la présence, pour la première fois, d'un stand du MEDEF à VivaTech cette année. L'objectif est de faire communiquer ces différents mondes pour qu'ils apprennent à mieux se connaître. Suite au rapport du BCG, nous avons identifié deux axes pour permettre à la France de renforcer sa position : tout d'abord multiplier les actions visant à gommer les disparités persistantes sur notre territoire en améliorant les compétences des Français par l'extension sensible du très haut débit, et en consolidant le rôle de catalyseur et de tiers de confiance joué par l'État, notamment pour les petites entreprises. Ensuite, rapprocher les pépites développant des solutions innovantes et les entreprises traditionnelles au sein des filières sectorielles, et former en masse des travailleurs du numérique compétents, capables d'exploiter le potentiel des nouveaux outils numériques dans ces organisations. C'est tout l'écosystème de l'entreprise qui doit se mobiliser et interagir. D'ailleurs, à leur niveau, les commissaires aux comptes ont une vraie responsabilité pour inciter leurs clients à prendre l'initiative.

Sur la question de la confiance numérique, vous préférez insister sur les opportunités que représente l'univers digital plutôt que sur les risques qui y sont associés. En quoi est-ce important d'appuyer sur ce point ?

C. P._ Le discours ambiant sur les dangers qui entourent le numérique est contre-productif car il n'y a pas une activité humaine où le risque est absent. Surtout, il sert de prétexte à ceux qui ne veulent pas affronter la réalité. De plus, il existe des réflexes simples et des bonnes pratiques qui peuvent être facilement mis en place pour mieux protéger son entreprise. Au-delà de la technique, la cybersécurité est une question de sensibilisation : l'important est que la cybersécurité soit traitée comme un sujet stratégique et pensée de manière globale.

« C'est tout l'écosystème de l'entreprise qui doit se mobiliser et interagir. D'ailleurs, à leur niveau, les commissaires aux comptes ont une vraie responsabilité pour inciter leurs clients à prendre l'initiative."

Quels outils le MEDEF met-il justement à disposition de ses adhérents pour appréhender au mieux les enjeux de confiance numérique ?

C. P._ Depuis quelques années nous avons lancé plusieurs dispositifs, dont le site cybersecurité.medef par exemple, qui propose quantité de conseils afin d'aider les dirigeants d'entreprise à y voir plus clair sur le sujet. Il y a un an, en partenariat avec les pouvoirs publics, nous avons ...

PHOTOS : DR

également lancé Alerte Cyber, qui vise à informer les TPE-PME, souvent esseulées dans la difficulté, sur les mesures reflexes à adopter en cas d'attaque cyber particulièrement critique. Lorsque celle-ci se produit, une notice succincte et compréhensible pour des non spécialistes de la cybersécurité est éditée par le dispositif national d'assistance aux victimes Cybermalveillance.gouv.fr et l'Agence nationale de la sécurité des systèmes d'information (ANSSI), puis adressée aux différents organismes interprofessionnels.

Comment les dirigeants doivent-ils appréhender la conduite du changement au sein de leur organisation ?

C. P._ C'est la problématique numéro un dans le monde de l'entreprise. Faire évoluer les organisations et les mentalités est un travail de longue haleine. On observe souvent des dirigeants d'entreprise qui ont saisi l'enjeu mais qui font face à un scepticisme interne. Or il est compliqué d'implémenter le changement sans l'appui des collaborateurs. Les nouvelles technologies impliquent des nouveaux usages qu'il faut absolument intégrer pour rester compétitif, par conséquent la communication, la formation et l'accompagnement sont des principes de management fondamentaux pour anticiper l'avenir et prévenir les tensions internes.

« Les nouvelles technologies impliquent des nouveaux usages qu'il faut absolument intégrer pour rester compétitif, par conséquent la communication, la formation et l'accompagnement sont des principes fondamentaux pour anticiper l'avenir et prévenir les tensions internes. »

Comme la CNCC, le MEDEF effectue une veille attentive des tendances à suivre lors d'événements comme le CES de Las Vegas ou VivaTech. Lesquelles avez-vous identifiées cette année ?

C. P._ Le sujet de la data est omniprésent. On ne compte plus les innovations qui s'y rapportent, mais le sujet d'après-demain, c'est le métavers. S'il est vrai que le phénomène est très « hype » et manque d'applications concrètes de grande ampleur, il occupe tous les esprits. Sur des secteurs comme le retail ou le luxe, il va se développer très rapidement. Un dirigeant d'entreprise ne peut pas se permettre d'observer ce phénomène de loin en pensant qu'il ne le concerne pas. Sur ce thème, comme sur celui de l'intelligence artificielle ou de la 5G, c'est le rôle du MEDEF de faire comprendre aux dirigeants d'entreprise dans quelle mesure cela va impacter leur activité.

Quelles doivent être selon vous les priorités du nouveau ministre délégué en charge de la transition numérique Jean-Noël Barrot ?

C. P._ Les priorités sont nombreuses. Au-delà de l'enjeu économique, les technologies au sens large, et en particulier le numérique sont indispensables pour décarboner nos activités de production, améliorer nos usages (télétravail, télémédecine, vente en ligne) et ainsi accélérer le développement d'une économie plus responsable. La planification numérique – qui concerne trois sujets majeurs : répondre au problème du manque de compétences, créer les infrastructures de pointe et maîtriser et valoriser les données – est une priorité absolue mais elle ne peut pas être de la seule responsabilité de la puissance publique. Les acteurs économiques comme les acteurs sociaux doivent nécessairement y être associés pour apporter leur vision, leur expertise et leur savoir-faire. ●

PHOTO : DR

PUBLICATION

Confiance numérique : crise ou transition ?

À travers les regards croisés de plusieurs experts, le dernier recueil de l'Institut Messine démontre à quel point le numérique interroge les enjeux de confiance.

Dans un monde marqué par la dématérialisation progressive de la valeur, la confiance numérique est devenue un facteur clé de croissance, et son manque un véritable frein. Pour toute organisation, l'enjeu est dès lors de mettre en place des systèmes à même de créer les conditions de cette confiance, en phase avec les attentes et les pratiques des individus. Un défi qui se révèle bien plus complexe qu'il n'y paraît. L'Institut Messine, le think tank de la profession de commissaire aux comptes créé avec le soutien de la CNCC, apporte sa contribution à cette indispensable réflexion avec la publication en mars 2022 d'un recueil intitulé *« La confiance à l'ère du numérique : cinq problématiques, six regards ».*

LA GOUVERNANCE DE LA DONNÉE, UN ENJEU ESSENTIEL

Cet ouvrage à l'approche originale s'appuie sur l'analyse de praticiens et d'experts aux points de vue complémentaires : entrepreneur, spécialiste du risque cyber, commissaire aux comptes, expert de la transformation des métiers du conseil, journaliste, essayiste… Chacun éclaire, depuis son poste d'observation, les bouleversements des enjeux de confiance à l'ère du numérique.

Leurs témoignages, mis en perspective, interrogent la question du juste équilibre entre une vision sacralisée de la confiance numérique, notamment autour de technologies comme la blockchain et les cryptomonnaies, ou au contraire, d'une méfiance disproportionnée, trouvant ses racines dans des risques bien réels.

Quelle que soit la position des dirigeants, la réalité est que les datas sont au cœur de l'économie numérique. Par conséquent, la confiance numérique suppose de prendre en compte la question de la gouvernance des données. Nathalie Malicet, membre du bureau national de la CNCC, rappelle que mal maîtrisé, le numérique peut avoir des effets adverses contre-intuitifs, exposant les organisations à de nouveaux risques. Garantir la confiance numérique représente par conséquent un défi essentiel pour tous les commissaires aux comptes, qui se retrouvent, au titre de leur activité d'audit et de certification des comptes, en situation d'émettre une opinion sur ces données. Mieux prendre en compte les enjeux de confiance numérique de leurs clients et les risques qui y sont liés, dans toute leur diversité, est un défi de taille pour tous les commissaires aux comptes. Un défi qui, s'il est relevé, est aussi une promesse d'avenir conclut l'Institut Messine : dans un monde de plus en plus irrigué par le numérique, la donnée et l'intelligence artificielle, la profession d'auditeur risque moins de disparaître que de voir son rôle renforcé. ●

Ci-dessus, **Frédéric Filloux** (grand reporter et chroniqueur à L'Express), **Ferghane Azihari** (essayiste et consultant en politiques publiques)**, Philippe Manière** (Institut Messine).

PHOTO : DR

Décryptage

CRYPTOACTIFS : UN ENJEU DE RÉGLEMENTATION ET DE VALORISATION

Du Bitcoin aux NFT, l'écosystème des cryptoactifs, indissociable de la technologie blockchain, questionne – bouleverse ? – l'environnement comptable.

Le numérique, et l'adaptation permanente qu'il impose au-delà d'une simple transformation, c'est aussi ce sentiment d'une accélération du temps. Dans cet environnement mouvant, la capacité d'adaptation des entreprises et de la profession des commissaires aux comptes aux nouveaux enjeux financiers susceptibles d'impacter leur activité est un enjeu crucial. Or, depuis plusieurs années, la crypto-économie et les technologies blockchain connaissent une croissance soutenue entraînant une vague d'innovations qui bouleversent les systèmes financiers et économiques traditionnels. Ces technologies sont au cœur de projets de transformation numérique de grande ampleur et constituent les fondations de nouvelles infrastructures de confiance. Leur capacité à préserver l'intégrité des données et à garantir une haute confidentialité dans les échanges les place comme des valeurs centrales au cœur de l'économie d'aujourd'hui et de demain. « À lui seul, le marché de la blockchain va représenter 37 milliards de dollars en 2025. C'est donc une réalité qu'il faut vite intégrer, insiste Rémy Ozcan, président de la Fédération des Professionnels de la Blockchain. À ce titre, les commissaires aux comptes auront un rôle clé à jouer dans la valorisation des actifs détenus par les entreprises dans le cadre de deal de fusion acquisition par exemple. » Encore faut-il maîtriser la réglementation et, pour commencer, le vocabulaire qui régit l'environnement des cryptoactifs *(cf. glossaire en page 18)*, une acculturation rendue d'autant plus nécessaire que leur encadrement fait, en France, l'objet de la plus grande attention du législateur.

LA FRANCE EN PREMIÈRE LIGNE

En adoptant la loi Pacte en 2019, la France a été l'un des premiers États à définir la notion « d'actif numérique » et à réguler certains sujets essentiels liés à l'écosystème de la technologie blockchain. L'apport majeur de la loi Pacte en la matière tient notamment à la création d'un régime encadrant les Initial Coin Offering (« ICO ») ou Offre au Public de Jetons, et l'activité des Prestataires de services sur actifs numériques (« PSAN »). En effet, le Code monétaire et financier (CMF) prévoit désormais que les prestataires souhaitant fournir en France des services de conservation, d'achat ou de vente d'actifs numériques en monnaie ayant cours légal, d'échange d'actifs

PHOTO : © PXHERE

numériques contre d'autres actifs numériques ou d'exploitation d'une plateforme de négociation d'actifs numériques, sont soumis à une obligation d'enregistrement préalable auprès de l'AMF. Dans l'examen de la demande d'enregistrement, l'AMF vérifie notamment que le PSAN se conforme aux obligations prévues par le CMF en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme (« LCB-FT ») et en matière de gel des avoirs. Ce nouveau régime permet ainsi de limiter les risques LCB-FT liés aux opérations portant sur des actifs numériques. Outre le fait qu'elle met fin au « Far West » dans lequel évoluaient jusqu'ici les acteurs du marché, le grand mérite de cette initiative est d'avoir mis en place un encadrement suffisamment contraignant pour réguler le système et apporter de la confiance vis-à-vis des utilisateurs finaux, mais sans limiter l'innovation, qui est un principe fondamental de l'écosystème numérique. Une confiance toute relative, avancent néanmoins certains, comme Aurore Lalucq, députée européenne et membre de la commission des affaires économiques et monétaires au Parlement européen. Celle-ci regrette que l'agrément qui accompagne l'enregistrement des PSAN auprès de l'AMF soit optionnel. Et ce alors qu'il est, selon elle, la condition sine qua non pour imposer de véritables normes en matière de transparence et de bonne gouvernance. L'idée fait malgré tout son chemin. Depuis deux ans, la Commission européenne est intervenue pour poser un cadre législatif commun d'encadrement du marché des cryptoactifs à l'échelle de l'Union européenne. D'abord avec le Digital Finance Package (DFP), publié en septembre 2020, puis avec le paquet LCB-FT contre le blanchiment, rendu public en juillet 2021. Dans le DFP, deux règlements concernent spécifiquement les cryptoactifs : le premier est le projet de règlement MICA (Market in Crypto Assets), adopté le 14 mars 2022 dernier par la commission des affaires économiques et monétaires du Parlement européen, qui ouvre la voie à l'entrée en vigueur du texte d'ici 2024.

LE POTENTIEL D'ATTRACTION DES CRYPTOACTIFS NE DOIT PAS ÊTRE BRIDÉ

Le second est le régime pilote pour les technologies de registre distribuées dans les infrastructures de marché (DLT). Celui-ci s'inscrit dans le cadre d'un ensemble de mesures de la Commission européenne visant à débloquer et à améliorer le plein potentiel du financement numérique pour l'innovation et la compétitivité. Le plan de financement numérique fournit une nouvelle stratégie visant à ce que le secteur financier de l'UE adopte et mène la révolution numérique avec l'aide d'entreprises européennes innovantes, de sorte que la finance numérique profite aux entreprises et aux consommateurs européens. Le texte sur le régime pilote portant sur la commercialisation des jetons de sécurité (c'est-à-dire les instruments financiers émis et/ou enregistrés dans une DLT/Blockchain) a lui aussi été adopté, permettant de supprimer les obstacles réglementaires à l'émission et à la négociation d'instruments financiers sur les réseaux blockchain. Dans un univers où les acteurs réclament un minimum de souplesse de la part des institutions pour ne pas brider le potentiel d'attraction des cryptoactifs, la confiance est l'enjeu central de la dynamique en cours et les commissaires aux comptes un rouage plus que jamais essentiel. ●

GLOSSAIRE

Airdrop (largage) : un airdrop survient lorsqu'une entreprise dépose des crypto-monnaies ou des NFT directement dans votre portefeuille. Contrairement à une introduction en bourse, les services de blockchain lancent un token et donnent aux gens qui ont utilisé le service par le passé. Cela peut arriver pour plusieurs raisons : pur marketing pour faire parler de ce token ou pour offrir des tokens de décision dans une DAO.

Aping : l'aping est l'action qui consiste à investir dans un token immédiatement après son lancement, sans prendre le temps de la réflexion, dans l'espoir de réaliser un profit à très court-terme.

Altcoin : toute crypto autre que le bitcoin ou l'ether. Certaines sont même baptisées shitcoin.

ANSSI : l'Agence nationale de la sécurité des systèmes d'information est chargée de proposer les règles à appliquer pour la protection des systèmes d'information de l'État et de vérifier l'application des mesures adoptées. Dans le domaine de la défense des systèmes d'information, elle assure un service de veille, de détection, d'alerte et de réaction aux attaques informatiques, notamment sur les réseaux de l'État. L'ANSSI apporte son expertise et son assistance technique aux administrations et aux entreprises avec une mission renforcée au profit des opérateurs d'importance vitale.

BCRCI : brigade centrale de répression de la criminalité informatique.

Binance : la plus grosse plateforme d'échange de crypto-monnaies, où les gens achètent et vendent des cryptos.

Blockchain : une blockchain est une base de données distribuée sur de nombreux systèmes informatiques de manière transparente, sécurisée, et fonctionnant sans organe central de contrôle. L'application phare de cette technologie est celle des crypto-monnaies.

Burn : un burn de crypto survient lorsque des cryptos sont envoyés vers des portefeuilles qui ne peuvent que les recevoir et non les envoyer. Ce genre de mécanisme est souvent utilisé pour son impact déflationniste.

Chiffrement : le chiffrement est un procédé de cryptographie grâce auquel on souhaite rendre la compréhension d'un document impossible à toute personne qui n'a pas la clé de (dé)chiffrement.

Chiffrement asymétrique : un chiffrement est dit asymétrique lorsqu'il utilise des clés différentes : une paire de clés (appelée biclé) composée d'une clé publique, servant à chiffrer, et d'une clé privée, servant à déchiffrer. Concrètement ce type de chiffrement permet deux choses distinctes que ne permet le chiffrement symétrique : Authentifier l'auteur/émetteur d'un message, d'une information, et chiffrer le message.

Chiffrement symétrique : un chiffrement est dit symétrique lorsqu'il utilise la même clé pour chiffrer et déchiffrer. C'est-à-dire que les différentes parties en présence doivent toutes connaître une même clé secrète, un même secret.

CNIL : la Commission nationale de l'informatique et des libertés est une autorité administrative indépendante française. La CNIL est chargée de veiller à ce que l'informatique soit au service du citoyen et qu'elle ne porte atteinte ni à l'identité humaine, ni aux droits de l'Homme, ni à la vie privée, ni aux libertés individuelles ou publiques.

Crypto-monnaie : une crypto-monnaie est une monnaie électronique basée sur les principes de la cryptographie pour valider les transactions et émettre la monnaie elle-même. Il existe de nombreuses crypto-monnaies : le bitcoin ou l'ether de la bockchain Ethereum.

Cryptographie : la cryptographie est une discipline s'attachant à protéger des messages (assurant

PHOTO : SHUTTERSTOCK

confidentialité, authenticité et intégrité) en s'aidant souvent de secrets ou clés. Le chiffrement et le déchiffrement sont des procédés de cryptographie.

Cyber-assurance : une cyber-assurance est une assurance proposant une protection contre des cyber-risques.

Cyber-risque : les cyber-risques sont l'ensemble des risques encourus par l'utilisation de l'informatique. On peut notamment citer les actes de malveillance informatique, les virus informatiques, le piratage informatique, le cyber espionnage économique ou industriel, le vol de données, les tentatives de cyber extorsion de fonds, les diffamations, injures, dénigrements sur Internet, l'usurpation d'identité.

DAO : organisation autonome décentralisée. Une DAO est une organisation dans laquelle les décisions sont prises par consensus : tous les possesseurs de jetons de gouvernance peuvent voter les décisions, celle qui a le plus de votes est retenue.

Délégué à la protection des données : le délégué à la protection des données est la personne chargée de contrôler la conformité au RGPD de l'organisme qui l'a désignée. Cette fonction est obligatoire pour les organismes exerçant des activités de profilage ou traitant des données sensibles à grande échelle.

Hameçonnage : vol d'identités ou d'informations confidentielles (codes d'accès, coordonnées bancaires) par subterfuge : un système d'authentification est simulé par un utilisateur malveillant, qui essaie alors de convaincre des internautes de l'utiliser et de communiquer des informations confidentielles, comme s'il s'agissait d'un système légitime ?

ICP : l'infrastructure de clés publiques est un outil cryptographique permettant de garantir l'authenticité des clés publiques par la signature électronique d'autorités de certification organisées de façon hiérarchique. Une ICP est l'un des outils fondamentaux d'une IGC.

IGC : une Infrastructure de gestion de clés est un ensemble organisé de composantes fournissant des services de gestion de clés cryptographiques et des certificats de clés publiques au profit d'une communauté d'utilisateurs.

Liquid market : un marché liquide est un marché avec énormément d'acheteurs et de vendeurs, ce qui permet d'acheter ou vendre presque immédiatement. Les marchés des crypto-monnaies sont liquides, les marchés de NFT ne le sont pas. La plupart des crypto-monnaies légitimes peuvent être achetées ou vendues n'importe quand, tandis que les NFT doivent être listés à la vente en espérant que quelqu'un les achète.

MiCA : voté le 14 mars par la Commission de la politique économique de l'Union européenne, le projet de règlement "Markets in Crypto-Assets", dit MiCA, fait partie du train de mesures sur la finance numérique, et contient un ensemble de dispositions visant à faire en sorte que le cadre réglementaire de l'Union applicable aux services financiers soit propice à l'innovation et n'entrave pas l'utilisation de nouvelles technologies.

Mining (minage) : le minage est le processus par lequel les transactions sont vérifiées et les blocs ajoutés à une blockchain. Cela implique généralement des machines puissantes capables de résoudre des problèmes de cryptographie complexes. C'est aussi de cette manière que de nouvelles crypto-monnaies sont mises en circulation.

Monnaie virtuelle : une monnaie virtuelle est un type de monnaie électronique non régulée qui est émise et contrôlée par ses développeurs, et utilisée et acceptée au sein de la communauté de ses utilisateurs.

NFT : le Nonfungible token ("Token non fongible") est un acte numérique qui certifie la propriété d'un actif numérique. À l'heure actuelle, ils sont principalement associés à l'art, mais les NFT peuvent certifier la propriété de n'importe quel bien numérique.

RGPD : le Règlement général sur la protection des données est un règlement européen relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. Il est applicable depuis le 25 mai 2018.

Token : les tokens sont des actifs de la blockain qui peuvent prendre des formes très différentes. Les crypto-monnaies comme le bitcoin sont un type de token. Il y a aussi les tokens de gouvernance, qui donne à son propriétaire un droit de vote dans une DAO ou les jetons utilitaires, où l'accès à un service est accordé selon le nombre de tokens détenus.

Ver (Worm) : un ver est un logiciel malveillant indépendant, cherchant à propager son code au plus grand nombre de cibles, puis de l'exécuter sur ces mêmes cibles ; il perturbe le fonctionnement des systèmes concernés en s'exécutant à l'insu des utilisateurs.

Le Mag

LES COMMISSAIRES AUX COMPTES,
bâtisseurs d'une société de confiance

www.cncc.fr

200/216 rue Raymond Losserand
CS 70044 75680 Paris Cedex 14
+33 (0)1 44 77 82 82