
DR
Yves LE QUERREC

Yves LE QUERREC
Président du Cos

Jean-François LEGENDRE
Rapporteur

Information **et communication numérique**


Le Cos, dans son périmètre, suit les dossiers liés à l'information : collecte, modélisation, structuration, sécurité…

Ralwel – Adobestock

Périmètre

Le Cos Information et communication numérique (ICN) couvre l'ensemble des questions autour du numérique, en particulier celles associées à la collecte ou la génération de l'information, sa structuration, sa modélisation, son traitement, sa diffusion, son stockage et sa préservation, ainsi qu'au traitement de la sécurité, physique ou immatérielle. Ce champ porte sur toutes les formes de communication – écrite, audiovisuelle, machine à machine… – et concerne toutes les formes d'échanges. Le Cos inscrit aussi son action dans un objectif d'écoresponsabilité et de contribution du numérique au développement durable.

La normalisation du numérique ambitionne de se situer à l'articulation entre un fournisseur et des clients afin de fournir des mécanismes volontaires de régulation facilitant l'ouverture des marchés, l'accompagnement des réglementations (en particulier les évolutions du cadre européen) et l'organisation des pratiques des acteurs du marché. Elle intervient pour faciliter la transformation de la société et permettre de nouveaux usages ainsi que pour faire le lien entre des aspects communication et information du M2M *(machine to machine)* et les aspects applicatifs des différents secteurs verticaux. Elle contribue à diffuser et valoriser l'innovation, vise un traitement unifié de la sécurité pour que des besoins d'interopérabilité de nature à améliorer l'efficacité des acteurs contribuant à la sécurité soient pris en compte.

Ses premiers utilisateurs sont des administrations, des fournisseurs de technologies : industriels, opérateurs et prestataires de services, des utilisateurs de ces services (dont les prescripteurs et les acheteurs), des consommateurs. Les normes du numérique concernent tout autant les sphères publiques que privées.

Les normes portent sur :

- Des technologies : équipements informatiques et télécommunications, logiciel, codage de l'information audiovisuelle, objets communicants (dont les capteurs), cartes à circuits intégrés, identification automatique, dispositifs optiques et tous supports (y compris le papier…).
- Des méthodes : l'ingénierie-système et les cadres d'architecture pour la conduite des projets complexes, la modélisation, la simulation, les langages, les syntaxes de structuration des contenus ou d'échanges de données, la représentation de données (dont l'information géographique et la géolocalisation), la qualité du logiciel et des services.
- Des services faisant appel à ces technologies : l'accès aux réseaux, l'informatique en nuage, l'enseignement et la formation à distance, l'e-administration, le commerce électronique, les ressources humaines, l'organisation de la sécurité, etc.
- L'organisation du numérique : la sécurité des échanges et la protection des utilisateurs, le management des contenus, les aspects légaux associés à leur localisation et leur accès ainsi que leur protection, l'identité numérique, l'écoresponsabilité et le développement durable, la mise en œuvre de systèmes ouverts.

Au-delà des spécificités du monde numérique, le périmètre intègre également, dans leur globalité et pour quelques domaines d'applications, la banque, la documentation, le secteur postal, l'espace et la sécurité du citoyen.

Les normes et les documents de référence contribuent à apporter des cadres génériques en appui aux travaux sectoriels fortement demandeurs : transport, santé, énergie… Les normes du numérique sont élaborées sur la scène internationale et européenne et, dans une moindre mesure, à l'échelle nationale. Des mécanismes appropriés facilitent une reconnaissance des meilleures spécifications issues de forums techniques. La normalisation soutient les besoins d'ouverture en matière d'outils et d'applications.

Contexte

Déjà pressentie comme une évolution majeure par le Cos dans les années passées, la transformation numérique de la société, notamment celle des entreprises, s'intensifie et confirme une véritable disruption, qui préfigure une 4e révolution industrielle.

Elle repose sur un socle de trois composantes incontournables et indissociables :

- Les objets connectés et les dispositifs dotés de capacités cognitives, qui fournissent un grand nombre de données numériques, dont les infrastructures physiques avec capteurs *(data fueling)* et, parmi les capteurs, les citoyens des villes ou districts intelligents (via les smartphones, etc.).
- Le traitement des mégadonnées en temps réel pour en tirer des analyses prédictives.
- Des infrastructures de services partagés, disposant de grandes capacités ubiquitaires pour en permettre l'exploitation. Les services de *cloud computing*, public, semi-public, privé constituent aujourd'hui une réalité incontournable.

Son développement s'avère générateur de fortes ambitions comme moteur de croissance, mais il suscite des craintes dans les usages compte tenu des risques avérés (cybercriminalité) et en raison d'éventuelles dérives : faux avis de consommateurs, exploitation abusive des données personnelles et des traces laissées sur les réseaux, fuite de données…

Les usages du numérique se développent massivement, sous la forme de logiciels traitant des données pour aider à la prise de

Zapp2photo – AdobeStock

Le management des contenus, les aspects légaux associés à la localisation participent de la nécessaire confiance numérique.

WaveBreakMediaMicro – AdobeStock

Parmi les documents importants publiés l'an dernier, plusieurs émanent de l'Iso/IEC et concernent les techniques de sécurité.

décision ou sous la forme d'objets pilotés par des outils numériques. Pour l'utilisateur, il est souhaitable que la normalisation intègre plus fortement la notion de transparence des principes sur lesquels les logiciels traitent les données : modèles utilisés, limite de validité des modèles, principe des traitements mis en œuvre (pour une prise de conscience de ce qui peut être ou non attendu du numérique).
La normalisation doit aider à développer une culture de la confiance à travers des pratiques partagées.
Les orientations 2017 du Cos contribuent à l'ensemble des huit thématiques transverses qui constituent la colonne vertébrale de la nouvelle Stratégie de normalisation française 2016-2018. Il joue de plus le rôle de référent de la thématique économie numérique.

Accompagner la mutation vers la digitalisation de l'entreprise et de la société

Développer l'exploitation des données massives

Les enjeux économiques, industriels, techniques et sociétaux associés à la collecte et l'exploitation de données de plus en plus massives sont importants. Ils représentent des opportunités, mais aussi des risques à appréhender, anticiper et maîtriser.
Les entreprises sont déjà engagées dans la refonte de leurs priorités stratégiques et de leur modèle opérationnel pour intégrer un ensemble combinatoire de progrès technologiques. L'un des points communs : l'archivage, le stockage et l'exploitation des données, avec leurs impacts en termes de communication et information. Ce sujet est au cœur des réflexions. Le besoin de travaux normatifs se fait chaque jour plus prégnant pour « canaliser » ce foisonnement.
En lien avec les lignes directrices apportées par le Livre blanc du Cos sur les données massives, les initiatives européennes, engagées dans le cadre des échanges franco-allemands, méritent d'être soulignées. Elles anticipent une évolution vers un concept d'intelligence de la donnée.

Soutenir le développement des objets connectés

En interconnexion avec le *big data*, les objets connectés sont nécessaires pour collecter la donnée et interférer avec l'environnement. Ce sujet porte sur un domaine extrêmement large : il concerne aussi les cartes et autres dispositifs d'identification et d'authentification, les équipements industriels (compteurs intelligents, réseaux domestiques, identification par radiofréquence, smartphones et autres tablettes), les nouveaux produits récemment commercialisés (montres, lunettes, tee-shirts). Pour autant, il convient d'assurer une cohérence conceptuelle et d'être à même de pouvoir raccrocher ce qui ressort des silos de données et ce qu'il est possible d'en faire dans le *big data*. Les sujets à traiter : la sécurité (dont la protection de la vie privée), les aspects physiques (la gestion de l'énergie, les applications sectorielles).
L'action du Cos vise à identifier les besoins d'interfaces et de normes génériques pour orienter les secteurs intéressés dans le développement de leurs spécifications. En parallèle, il soutient le développement en cours de normes internationales suffisamment génériques pour permettre un niveau d'harmonisation qui tienne compte de multiples

NORMES ET DOCUMENTS NORMATIFS IMPORTANTS PUBLIÉS EN 2016

NF Iso/IEC 27000	Technologies de l'information – techniques de sécurité – systèmes de gestion de sécurité de l'information – vue d'ensemble et vocabulaire
NF Iso/IEC 27009	Technologies de l'information – techniques de sécurité – application de l'Iso/IEC 27001 à un secteur spécifique – exigences
Iso/DIS 12812-1	Opérations bancaires de base – services financiers sur mobile – partie 1 : cadre général
NF Iso 2108	Information et documentation – numéro international normalisé du livre (ISBN)
NF Iso 15489-1	Information et documentation – gestion des documents d'activité – partie 1 : concepts et principes
NF Iso 11799	Information et documentation – exigences pour le stockage des documents d'archives et de bibliothèques – information et documentation – prescriptions pour le stockage des documents d'archives et de bibliothèques
NF Iso 30302	Information et documentation – système de gestion des documents d'activité – lignes directrices de mise en œuvre
NF Iso/IEC 30134-2	Technologies de l'information – centres de données – indicateurs de performance clés – partie 2 : efficacité dans l'utilisation de la puissance (PUE)

Il s'implique dans la normalisation…


DR

Vincent STRUBEL

Sous-directeur expertise à l'Agence nationale de la sécurité des systèmes d'information (Anssi).

Comment, au cours de l'année écoulée, s'est caractérisé votre investissement dans les travaux de normalisation ?
Au-delà du travail de veille et de suivi de nombreux projets et groupes de travail, y compris sectoriels, l'Anssi a pris, en janvier 2016, la coprésidence d'une task force *créée au sein de la commission de normalisation SSI d'Afnor, dans le cadre de la révision des normes internationales relatives aux critères d'évaluation pour la sécurité des technologies de l'information (normes Iso 15408 et Iso 18045). L'Agence a ainsi apporté son expertise et son savoir-faire en matière de certification des produits de sécurité, en participant, aux côtés des acteurs français concernés, aux négociations internationales menées dans le cadre de l'Iso. Ces travaux se poursuivent cette année, toujours avec le soutien de l'Agence.*
L'Anssi anime par ailleurs un groupe d'experts en charge de définir et promouvoir la position française en matière de signature électronique au sein du Cen/TC 224/WG 17. L'Agence est à ce titre éditrice d'un profil de protection sur la signature à distance dans le cadre de ce groupe de travail européen. Ces travaux revêtent une importance primordiale dans la mesure où ils s'inscrivent dans le cadre du règlement européen eIDAS sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur.
L'Anssi fédère également une communauté d'industriels participant aux travaux du Trusted Computing Group (TCG), dont l'objectif est de faire émerger des technologies de sécurité utilisables dans différents types d'équipements informatiques.
Enfin, l'Agence apporte un soutien ponctuel aux différents acteurs français impliqués dans les travaux de normalisation dans les domaines relevant de son expertise.

Quelle est la stratégie de votre organisation pour les années qui viennent en matière de normalisation ?
La Stratégie nationale pour la sécurité du numérique, présentée par le Premier ministre le 16 octobre 2015, a fait de la normalisation un enjeu majeur dans le cadre de la mise en place d'une véritable autonomie stratégique numérique en Europe. Le partenariat public-privé européen lancé par la Commission européenne le 5 juillet 2016 et entièrement dédié à la cybersécurité a également fait du développement et de l'usage de normes européennes un objectif prioritaire de ces prochaines années. L'Anssi entend donc poursuivre son action et renforcer son investissement en matière de normalisation, en étroite collaboration avec l'ensemble des acteurs concernés, aussi bien dans le cadre d'Afnor qu'au sein du Comité de la filière industrielle de sécurité (Cofis) ou dans le cadre des relations que nous entretenons avec nos partenaires français et étrangers.
Par ailleurs, les sujets sur lesquels l'Anssi va particulièrement s'investir sont d'une part ceux qui soutiendront la certification de sécurité à l'échelle européenne, qu'il s'agisse de produits ou de services, dans un contexte certes international, mais préservant le fort acquis national, notamment en matière de labellisation des prestataires ; d'autre part ceux relatifs à la sécurité des protocoles, notamment cryptographiques, pour favoriser un Internet des objets sûr, à l'échelle mondiale de préférence ; et enfin les travaux autour de la mise en œuvre des directives et règlements européens dans les domaines de l'identification électronique et des services de confiance (eIDAS), de la sécurité des réseaux et des systèmes d'information (NIS) ou encore de la protection des données à caractère personnel (règlement GDPR).

En quoi les mécanismes collectifs de normalisation peuvent-ils aider à répondre aux défis qui se posent à votre organisation ?
L'Anssi participe aux différentes instances de concertation et de coordination nationales en matière de normalisation dans les domaines de la SSI et de la cybersécurité (commissions Afnor, sous-commission normalisation du Cofis). Cette coordination est plus que jamais indispensable à l'heure où les enceintes de normalisation dédiées à la cybersécurité ou sectorielles mais incluant un volet sécurité prolifèrent et alors que certains pays consacrent des moyens nettement supérieurs aux nôtres à la normalisation. Il est donc primordial de définir collectivement nos priorités, d'essayer dans la mesure du possible de concilier nos stratégies, afin de répartir la charge de travail entre les acteurs impliqués et de coordonner nos actions le plus en amont possible.
L'avènement d'une norme étant souvent le fruit d'un travail préalable de sensibilisation, de persuasion et d'influence, il faut pouvoir renforcer nos mécanismes de veille et d'alerte afin d'anticiper les travaux et identifier les experts qui pourront in fine travailler à l'élaboration de la norme. Cette capacité d'anticipation est aujourd'hui indispensable, notamment dans le cadre de l'élaboration des réglementations européennes, dont certaines peuvent s'appuyer sur des normes qui doivent pouvoir préserver nos intérêts.
Enfin, le recours à des logiciels libres de sécurité dans de nombreuses implémentations fait de ces derniers de véritables standards de fait. C'est pourquoi l'Anssi s'est positionnée activement dans ce domaine.

Comment appliquez-vous les normes qui concernent votre organisation ?
L'une des missions de l'Anssi consiste en l'élaboration et la publication de guides et référentiels d'exigences techniques et organisationnelles dans les domaines de la SSI et de la cybersécurité. À ce titre, la connaissance de l'état de l'art et des normes applicables dans les domaines d'expertise de l'Agence est une condition indispensable à l'exercice de nos missions. De nombreuses normes ou spécifications techniques européennes et internationales sont ainsi référencées dans les documents publiés par l'Anssi. À titre d'exemple, les référentiels d'exigences applicables aux prestataires de détection (PDIS) et de réponse aux incidents de sécurité (PRIS) s'appuient sur les travaux du groupe de travail sur les indicateurs de sécurité de l'Etsi. Le référentiel applicable aux prestataires d'audit de la SSI (PASSI) référence quant à lui de nombreuses normes issues du sous-comité (SC) 27 de l'Iso/IEC/JTC 1 relatif aux techniques de sécurité des technologies de l'information. Les experts de l'Anssi sont donc consommateurs de nombreuses normes issues de l'Iso, de l'Etsi, du Cen-Cenelec ou de l'IEC comme d'autres organismes

tels que l'OACI ou l'AIEA pour des spécifications ou normes sectorielles.
L'application obligatoire de normes ou spécifications techniques dans le cadre de la mise en œuvre de réglementations européennes qui s'imposent aux entreprises et aux citoyens appelle par ailleurs à renforcer notre vigilance dans leur élaboration.

De nouveaux paramètres interfèrent-ils dans vos réflexions et travaux ?
L'élaboration et la mise en œuvre de réglementations nationales et européennes dans les domaines de l'identification électronique et des services de confiance (référentiel général de sécurité, règlement eIDAS), de la sécurité des réseaux et des systèmes d'information (loi de programmation militaire, directive NIS) ou encore de la protection des données à caractère personnel (règlement GDPR) incitent de plus en plus, pour l'Anssi notamment, à anticiper et à s'impliquer le plus en amont possible dans l'élaboration de normes et spécifications techniques sur lesquelles pourront s'appuyer ces différentes réglementations.
Dans ce cadre, l'influence sans cesse croissante des forums et consortiums internationaux, tout comme la prolifération de groupes de travail – y compris sectoriels – ou plateformes consultatives liés à la normalisation dans les domaines de la SSI et de la cybersécurité imposent aux acteurs français et européens de renforcer leur coopération le plus en amont possible. L'Anssi a ainsi, au cours de ces dernières années, renforcé sa coopération avec l'Allemagne en matière de normalisation, ce qui a par exemple conduit à l'élaboration conjointe et à la promotion à l'international de spécifications techniques relatives à un support physique (Token) pouvant répondre aux exigences du règlement européen eIDAS. Cette coopération franco-allemande se poursuit actuellement dans le cadre des travaux conduits par le Cen/TC 224/WG 17.
Les réflexions et travaux prochainement entrepris en matière de normalisation dans le cadre du partenariat public-privé européen dédié à la cybersécurité nous imposeront de renforcer et d'étendre cette coopération à d'autres partenaires.

Organisme : Anssi
Domaine d'activité : sécurité des systèmes d'information.
Taille : 500 personnes.


Tomasz Zajda – AdobeStock

Le sous-comité Iso/IEC/JTC 1/SC 27 dédié à la sécurité de l'information a déjà produit des normes mondialement utilisées.

initiatives prises à différents niveaux : protocoles, architectures, intégrité des données, etc. En Europe, il faut suivre attentivement l'initiative the Alliance for Internet of Things Innovation (AIOTI), dont un aspect concerne la normalisation.

Développer la normalisation autour du dispositif blockchain

Le Cos a identifié le *blockchain* comme une technologie de rupture pouvant constituer une réponse pour la traçabilité de transactions de toute nature. Cette technologie s'appuie sur un dispositif distribué de vérification des chaînes associées aux transactions. Il existe de nombreuses initiatives, et les cas d'usage se multiplient. Ils ne se limitent pas, loin s'en faut, à la monnaie virtuelle.
Cependant, les enjeux normatifs liés à cette technologie de rupture sont importants et se traduisent en termes de vocabulaire et d'ouverture, de sécurité, d'interopérabilité, de gouvernance, d'indépendance des solutions et d'adaptation aux besoins des cas d'usage.
Le Cos se propose d'étudier en détail ces sujets afin d'organiser les actions qui faciliteront la mise en place d'un dispositif de normalisation approprié.

Définir les exigences permettant la transition numérique du document

L'un des enjeux essentiels de la transformation numérique est d'assurer une continuité entre le matériel et l'immatériel sous les aspects techniques, en appui des réglementations.
Plusieurs dispositions sont envisagées pour y parvenir et peuvent d'ailleurs être utilisées de façon combinée. La signature électronique peut être intégrée dans une facture électronique. Le cachet électronique visible apposé à un justificatif garantit les données contenues dans le cachet qui se présente sous forme d'un code optique à deux dimensions. Ce dispositif s'appuie également sur une signature numérique pour en assurer l'authenticité.
En matière d'archivage de l'information, l'enjeu normatif concerne désormais la numérisation fidèle des documents, qui permettra de faire le pont entre le document à valeur probante sous forme numérique et son équivalent matérialisé.
Le besoin s'exprime de disposer de normes internationales, et la France a la capacité d'être force de proposition : elle a déjà pris l'initiative en portant sur la scène internationale le format d'échange Medona (norme NF Z 44-022).

Solliciter et diffuser une culture de la qualité dans les services numériques

Les bénéfices technologiques et économiques du *cloud* sont unanimement reconnus : en simplifiant l'accès aux données, l'accompagnement des entreprises face aux enjeux de développement et de mobilité se trouve facilité.
En lien avec les différentes initiatives gouvernementales ou régionales, l'action du Cos s'oriente vers un soutien aux éditeurs et fournisseurs de services par le développement d'une déclinaison de la normalisation adaptée à la transition vers l'informatique en nuage des PME. Pour aider cette transformation numérique, véritable exigence, le Cos est particulièrement attentif à la bonne prise en compte de la normalisation et des normes déjà existantes par des travaux destinés à

Il s'implique dans la normalisation…


DR

Pascal PAILLIER

Expert senior en sécurité et président de CryptoExperts.

Comment, au cours de l'année écoulée, s'est caractérisé votre investissement dans les travaux de normalisation ?
L'essentiel de mes travaux ont lieu au sein du sous-comité (SC) 27 de l'Iso/IEC/JTC 1, là où les normes internationales en matière de sécurité de l'information sont débattues et rédigées. Le SC 27 est notamment connu pour sa série de normes Iso/IEC 27000, qui visent le management de la sécurité, mais aussi pour la norme Iso/IEC 15408 Critères communs, par exemple. Une partie des travaux du SC 27 est également consacrée à l'émergence de normes sur l'identité et la gestion des données personnelles. Mais le groupe de travail du SC 27 dans lequel je suis le plus investi est celui qui se consacre à la mise au point des normes de cryptographie, le working group (WG) 2. Il est essentiellement composé de cryptologues reconnus issus des milieux académiques, industriels ou gouvernementaux, et qui souvent mènent aussi une activité de recherche scientifique dans le domaine. Peu d'États membres sont activement représentés dans ce groupe de travail (environ une quinzaine seulement), mais la France a toujours réussi à y maintenir une présence, même si nous n'y sommes actuellement que deux ou trois experts et si un renforcement serait le bienvenu. Outre le suivi de l'ensemble des activités du WG 2, je suis l'éditeur principal d'une norme sur le chiffrement homomorphe, un mécanisme cryptographique qui va probablement s'avérer fondamental dans la sécurisation du cloud. J'espère aussi pouvoir lancer prochainement un nouveau projet de norme dédié à l'authentification anonyme, mécanisme par lequel une entité (humain ou dispositif) prouve à un fournisseur de service qu'elle est autorisée à accéder à son service sans toutefois révéler son identité complète. Là aussi, la cryptographie est particulièrement en avance sur les usages. L'ensemble des contributeurs français au SC 27 se réunissent en France au sein d'un comité miroir animé par Afnor : la commission de normalisation (CN) 27 SSI. Présidée par Jean-Pierre Quémard, doté d'une grande expérience, la CN regroupe des experts de tous les domaines de la SSI, capables de formuler les enjeux nationaux défendus ensuite à l'Iso par la délégation qui y est envoyée. C'est un groupe ouvert et particulièrement proactif. On le doit largement à l'engagement constant d'Afnor, à travers le secrétaire de la CN 27 SSI, Frédéric Solbes. C'est un plaisir toujours renouvelé de travailler avec ce groupe de personnalités impliquées et enthousiastes, ce qui ne peut qu'aider face à l'ampleur de la tâche !

Quelle est la stratégie de votre organisation pour les années qui viennent en matière de normalisation ?
CryptoExperts est une société indépendante qui met au point des solutions de cryptographie avancée qui vont bien au-delà des problématiques usuelles du chiffrement et de la signature numérique. Des collaborateurs remarquables partagent avec moi cette aventure. Depuis notre création en 2009, nous avons compris que l'émergence sur le marché de nouvelles technologies de cryptographie ne pourrait se faire sans une large adoption industrielle qui devait parfois passer par la normalisation. Prenons l'exemple du chiffrement homomorphe, qui permet de calculer sur des données chiffrées sans avoir à les déchiffrer. Cette technologie n'existe que depuis quelques années dans une forme réellement utilisable. Chacun entrevoit là un potentiel industriel énorme, mais derrière la « guerre des brevets » et la multitude d'options dans les réalisations techniques possibles, l'industrie a besoin d'un guidage avant d'investir avec confiance dans le développement de solutions pérennes. La normalisation vient précisément combler ce besoin. Au-delà, nous souhaitons tout simplement contribuer à faciliter l'émergence des nouvelles technologies cryptographiques, dont il est évident que l'industrie de la sécurité (et à plus long terme la société) aura de plus en plus besoin. Une part de cette motivation est stratégique : nous nous préparons à bénéficier de ces avancées, en tant que fournisseur de solutions. Mais cette motivation est aussi sincèrement désintéressée. Il s'agit de mettre notre expertise au service d'un écosystème complexe, celui qui relève de la sécurité numérique des personnes et des biens (au sens large), et j'y vois une extension naturelle de l'objet social de CryptoExperts : contribuer à une société plus sûre.

En quoi les mécanismes collectifs de normalisation peuvent-ils aider à répondre aux défis qui se posent à votre organisation ?
Les défis auxquels CryptoExperts fait face en normalisation sont assez largement partagés par beaucoup d'autres organisations opérant dans la sphère de la sécurité des données et du respect de la vie privée. Il s'agit, pour une large part, d'aider à faire évoluer tout un écosystème d'acteurs vers de meilleures solutions qui auront un réel impact sur la vie des citoyens. Pour nous, l'ennemi est l'inertie industrielle, qui s'explique dans une large mesure par la méconnaissance des nouvelles potentialités d'innovation qu'offre la cryptographie d'aujourd'hui. Il s'agit d'accréditation anonyme, du crypto-calcul collaboratif, d'obfuscation cryptographique ou des algorithmes post-quantiques. Elles feront, à terme, partie intégrante de notre futur, comme les cryptomonnaies et la blockchain aujourd'hui. En contribuant à la normalisation en matière de cryptographie, nous ne recherchons pas nécessairement d'avantage concurrentiel, mais plutôt à enrichir l'écosystème. Dans notre domaine, la normalisation doit permettre l'émergence de solutions nouvelles sans faire peser de contrainte sur les précédentes. Exemple typique : une norme de cryptographie dite « avancée » comme l'Iso/IEC 20008 pour les signatures anonymes ne rend pas obsolète la signature numérique classique, mais l'enrichit pour y permettre un anonymat partiel du signataire. À long terme, les technologies de signature anonyme prendront probablement le pas sur la signature classique, en tout cas pour un certain nombre d'usages dans lesquels le respect de la vie privée du signataire est nécessaire ou préférable. Les normaliser rend possible de nouvelles opportunités commerciales pour de nombreux acteurs du marché de la signature et de l'identité. CryptoExperts bénéficie déjà d'un large réseau de partenaires dans le cadre de ses activités de recherche collaborative, mais apprécie toujours de nouveaux rapprochements. Mener des travaux de normalisation est une façon privilégiée de faire de nouvelles rencontres. Le monde de la SSI est finalement très petit !

Comment appliquez-vous les normes qui concernent votre organisation ?
Pour l'essentiel, les normes de cryptographie spécifient des mécanismes sous forme d'algorithmes ou de protocoles bien précis. Nous les implémentons dans les produits et services développés pour nos clients. Souvent, lorsque la conformité à une norme est optionnelle pour un client, nous essayons tout de même de nous en approcher au maximum dans l'esprit. Les normes sont souvent bien faites !

Quel est le retour sur investissement, matériel et surtout immatériel, de votre mobilisation ?
Je suis partiellement financé par des projets de recherche pour mes déplacements et le temps passé en normalisation. Le crédit impôt recherche (CIR) prend aussi en charge une partie de ces coûts. Pour le reste, il s'agit pour ma société d'offrir mes services pour la bonne cause ! Ce n'est pas si inhabituel au sein des PME : elles y sont incitées par plusieurs mécanismes nationaux, européens ou internationaux et aussi parfois par déontologie professionnelle. Certains de mes collègues en commission de normalisation sont aussi des dirigeants d'entreprise animés de cette même passion.
Les coûts résiduels de mes travaux s'avèrent donc modiques pour CryptoExperts. En revanche, nous y gagnons sur plusieurs terrains. Intérêt immédiat : je connais très bien tous les standards cryptographiques de l'Iso, ce qui s'avère fort utile dans mes activités de conseil et de R&D. À plus long terme, l'intérêt est aussi de pouvoir suivre les tendances et même les anticiper avec nos propres solutions. La communication véhiculaire typiquement (ce que l'on appelle le V2V, V2C, V2X, etc.) va certainement évoluer vers des signatures numériques spéciales, car les voitures ont besoin de vérifier en temps réel l'authenticité d'un grand nombre de messages entrants provenant des sources environnantes. Dès lors, nous pouvons déjà chercher à concevoir des signatures à même d'être vérifiées en grand nombre simultanément plutôt qu'une par une et mettre au point un plan de valorisation d'une telle solution. Je pourrais citer de nombreux autres exemples. Notre retour sur investissement tient à l'acquisition d'une certaine capacité à identifier de nouvelles opportunités.

Voyez-vous poindre dans votre activité de nouveaux défis en termes de normalisation auxquels vous n'étiez jusqu'alors pas confronté ?
Oui bien sûr ! Le groupe de travail sur la cryptographie au SC 27 est confronté à au moins deux défis grandissants. Il s'agit d'abord de pouvoir normaliser des mécanismes crypto qui apportent une aide immédiate aux autres communautés de la SSI. Les experts de la sécurité du cloud, *par exemple, ont besoin de nouveaux outils comme le chiffrement homomorphe dans la conception de leurs architectures. Le* privacy-by-design *et l'IoT formulent également des besoins auxquels nous devons apporter des réponses normatives adaptées : l'authentification anonyme et cryptographie* lightweight. *Ces besoins apparaissent spontanément autour de nous (au WG2) et sont de plus en plus nombreux. Avec la récente création d'un nouveau sous-comité dédié à la* blockchain, *il est probable que le WG 2 soit invité à réfléchir aux outils crypto qu'il peut proposer dans ce domaine.*
Simultanément, il existe une menace transverse à toutes les applications de la cryptographie : l'apparition prochaine des processeurs quantiques. Cette révolution annoncée est une catastrophe pour la cryptographie actuelle : les niveaux de sécurité des mécanismes vont soudain s'écrouler. Pour le grand sceptique du calcul quantique que je suis, il est douloureux d'apprendre que tous les ingrédients technologiques qui constituent un ordinateur quantique sont déjà à peu près maîtrisés et qu'à horizon de dix-quinze ans, cet ordinateur se retrouvera sur mon bureau et celui de millions d'autres. Sans parler des agences de renseignement comme la National Security Agency (NSA), qui bien sûr, seront équipées avant tout le monde. Il faut savoir que la communauté scientifique n'est aujourd'hui pas unanime quant au choix des mécanismes cryptographiques de remplacement (dits « quantum-safe » ou « post-quantiques »). Lorsqu'on connaît les temps de cycle en normalisation, il est temps de s'y intéresser. C'est pourquoi l'Iso, mais aussi l'IETF, l'Etsi et surtout le Nist ont ajouté récemment ce sujet critique à leur plan de travail. Mais à ce stade, tout reste encore à faire…

La crise économique à laquelle nous sommes confrontés modifie-t-elle votre regard vis-à-vis de l'action collective que constitue la normalisation ?
Les enjeux de sécurité numérique sont peu affectés par la crise économique, en tout cas pas autant que par les évolutions techniques, normatives et réglementaires.
En revanche, de nombreux indicateurs montrent que nous vivons dans un monde numérique relativement peu sûr. L'on peut parler de crise sécuritaire mondiale. À mon sens, c'est plutôt cette crise-là qui remet en perspective la normalisation des techniques de sécurité, car l'on peut constater qu'elle est largement insuffisante : bien que nous disposions de tout ce qu'il faut en matière de normes de chiffrement, d'authentification et de gestion de clés, qui utilise aujourd'hui du véritable chiffrement end-to-end *? L'utilisateur est facilement trompé par des applications comme Telegram, Signal ou Whatsapp, qui se présentent comme telles, mais conservent en réalité une copie des clés, sur leurs serveurs ou ailleurs. En matière de courriels, peu de gens utilisent vraiment PGP/GPG en pratique, et la norme S/MIME n'est pas assez flexible pour permettre un chiffrement de courriels par défaut entre utilisateurs.*
Cet état de fait est assez décevant : il montre que tous les efforts pour la normalisation de la cryptographie ne garantissent même pas une sécurité de base acceptable dans les communications quotidiennes.
Cette observation s'accompagne d'une prise de conscience croissante et heureusement assez générale de la part des opinions publiques. En France, l'Agence nationale de sécurité des systèmes d'information (Anssi) véhicule des recommandations auprès des entreprises, des institutionnels et du grand public en faisant des risques numériques « l'affaire de tous ». Un message de vérité indispensable et œcuménique de la part d'une Agence dont le président se trouve être, lui aussi, cryptologue !

Organisme : CryptoExperts
Domaine d'activité : recherche et développement en cryptographie.
Taille : TPE.

créer un espace de confiance européen et à garantir un traitement sécurisé des données.
Il convient de veiller à ce que les différents standards et normes en cours d'élaboration ou déjà disponibles assurent la complétude des besoins.

Contribuer au renforcement de la sécurité du citoyen et soutenir le développement de la confiance

Harmoniser les interfaces, données et procédures, comme le requiert la sécurité des personnes

L'une des priorités politiques de nos sociétés est la lutte contre le terrorisme, la gestion des flux migratoires, la résilience des populations aux catastrophes… L'efficacité de la réponse des autorités en charge de cette mission de base se trouve handicapée par le morcellement des acteurs et l'incompatibilité de leurs moyens.
Dans un contexte où sécurité physique et numérique sont de plus en plus liées, la prise en compte par la normalisation de ces besoins vitaux est devenue une urgence sociétale à intégrer en complément des normes techniques en place et en cohérence avec elles. En d'autres termes, si les parties prenantes disposent en général des règles leur permettant de fonctionner harmonieusement dans leur environnement, l'objectif est de développer les moyens pour que ces environnements puissent échanger nativement, en particulier dans les situations d'urgence.

Contribuer à la mise en place d'une identité numérique

La dépossession des personnes de leurs données et de la maîtrise de leur environnement numérique, le risque relatif à la réputation des entreprises, les pratiques déloyales sur les réseaux sont des facteurs pour lesquels le numérique modifie la chaîne de valeur. Ces comportements constituent d'importantes questions quant à leur interférence avec le développement des échanges électroniques.
Pour autant, la numérisation offre de nouvelles opportunités de redéfinir les concepts modernes de l'identité, avec des entités fragmentées qu'il est possible sous certaines conditions de fédérer.
Une identité fiable et de confiance permettra d'ouvrir vers de nouvelles prestations de services clés :

- services financiers de détail : offres de crédit confortées par la fourniture de données vérifiables et de confiance ;
- assurances : renseignements personnels vérifiés pour permettre l'évaluation des risques et la tarification des produits d'assurance à une plus grande résolution que possible actuellement ;
- éducation : vérification des qualifications et des expériences pour protéger les diplômes et le cursus au moment où le modèle des cours massifs en ligne se développe à grande échelle ;
- services médicaux : intégrité de l'identité individuelle, élément fondamental des dossiers médicaux.

Il est donc important d'apporter des réponses pragmatiques aux enjeux du commerce électronique qui permettent de redonner un sens à l'expérience client tout en prouvant aux utilisateurs que leurs données seront exploitées de façon conforme à leurs attentes.
L'ensemble des solutions et des systèmes d'informations existants doivent et devront répondre à des critères de confidentialité et de sécurité des données partagés. L'identité numérique devient l'un des éléments de cette sécurité à prendre en compte dans le cadre du règlement européen e-IDAS. L'identité numérique est en outre une clé d'entrée pour développer des services numériques de confiance et accélérer la transformation numérique de la société.

Redonner à la personne le pouvoir sur ses données à caractère personnel

Le Cos va soutenir les initiatives des acteurs français destinées à apporter des solutions aux enjeux internationaux et européens en matière de protection de la vie privée, en relation notamment avec les priorités communautaires et la nouvelle réglementation GDPR approuvée par le Parlement européen en avril 2016.
En cohérence avec l'ensemble des sujets évoqués (dont le *big data*), l'objectif est de redonner aux personnes le droit de contrôler l'usage de leurs données personnelles et de réconcilier les citoyens avec la galaxie des services auxquels ils ont accès en laissant des traces, tout en facilitant les transactions et l'exploitation des données par les acteurs de la chaîne de valeur.

Coordonner la normalisation des paiements

L'acte de paiement est incontournable dans le processus commercial et dans le commerce électronique. Il existe actuellement une mosaïque de solutions, qui varient en fonction de multiples facteurs. Ces solutions sont hétérogènes, parfois propres à un domaine, voire à un commerce donné. En revanche, tout le monde s'accorde sur l'absence et donc la nécessité d'établir des solutions universelles.
Pour établir une stratégie normative, plusieurs questions essentielles se posent : comment simplifier l'approche paiement sur le plan technique ? Comment le rendre « agnostique » des solutions logicielles ? Des travaux sont-ils envisageables dans ce périmètre de la couche intermédiaire navigateur-applicatif serveur ou OS-applicatif dans le cas de l'Internet des objets pour élaborer un ensemble de dispositifs universels ? Faut-il intégrer un volet sur les réseaux sociaux positionnés désormais sur ces questions ?

Renforcer la cybersécurité

Les enjeux de la normalisation cybersécurité sont bivalents : ils comprennent une dimension de soutien à l'industrie française

NORMES ET DOCUMENTS NORMATIFS IMPORTANTS PRÉVUS EN 2017

Iso/IEC 27003	Technologies de l'information – techniques de sécurité – lignes directrices pour la mise en œuvre du système de management de la sécurité de l'information
Iso/IEC 27007	Technologies de l'information – techniques de sécurité – lignes directrices pour l'audit des systèmes de management de la sécurité de l'information
Iso/IEC 27011	Technologies de l'information – techniques de sécurité – lignes directrices du management de la sécurité de l'information pour les organismes de télécommunications sur la base de l'Iso/IEC 27002
Iso/IEC 27021	*Information technology – security techniques – competence requirements for information security management systems professionals*
Cen/TS 17073	Services postaux – interfaces pour les colis transfrontaliers
NF Iso 3901	Information et documentation – code international normalisé des enregistrements (ISRC)
NF Iso 20614	Protocole d'échange de données pour l'interopérabilité et la préservation
Iso/IEC CD 20546	*Information technology – big data – definition and vocabulary*


Psphotography – AdobeStock

Les données personnelles concernent évidemment des sujets sensibles (santé), alors que la mise en œuvre du règlement européen GDPR s'amorce.

de sécurité qui se traduit par une capacité à mettre en place des infrastructures de confiance de haut niveau et le besoin de sensibiliser le tissu économique à l'intérêt de la normalisation. Pour cela, il convient de proposer des bonnes pratiques immédiatement exploitables par les entreprises.
Dans la sécurité, les pouvoirs publics ont un rôle important. Le Cos est attentif à la cohérence du dispositif européen en matière de normalisation afin d'assurer une bonne coordination des travaux et de limiter la multiplication d'instances traitant de normes et standards de cybersécurité. La pertinence de reprendre sous forme européenne des normes internationales, stratégie poussée par l'Allemagne, est à étudier au cas par cas. En effet, limiter l'organisme de normalisation européen à une chambre d'enregistrement de normes internationales n'apporterait qu'une très faible valeur ajoutée au regard des besoins exprimés par les parties intéressées. Il convient plutôt de miser sur la complémentarité en Europe et à l'international et de pousser au développement des normes dont l'Europe a besoin, en particulier en appui à des réglementations et particulièrement la nouvelle directive NIS.
Côté international, le Cos veille à la pertinence et à la qualité des interfaces entre les différentes commissions de normalisation impliquées. Pour promouvoir l'intégration d'une approche globale et cohérente de la normalisation des référentiels qui touchent à la gestion la sécurité numérique dans les stratégies normatives des secteurs, le Cos accompagne la réflexion quant à la coordination des travaux en matière de sécurité relevant de différents organismes, Cen, Cenelec, Iso, Etsi, avec en filigrane la perspective de saisir les opportunités qui se présenteraient pour les acteurs français de se positionner.

Accompagner la compétitivité des filières et la performance de l'économie française

Les domaines d'application

Il est important d'asseoir la démarche de développement d'un ensemble cohérent de normes génériques s'appuyant sur l'existant et permettant d'assurer plusieurs fonctions fondamentales : interopérabilité, sécurité, généricité et adaptabilité aux cultures et aux besoins spécifiques, mais aussi intégration d'objectifs environnementaux. Pour cela, le Cos s'appuie sur les domaines métiers qui entrent dans son périmètre ainsi que sur des cas d'usage :

- les *smart cities*, y compris la ville numérique, les réseaux intelligents et la *smart* mobilité, la création de ressources partageables, l'intelligence collaborative, la gestion des données confort et l'intégration des seniors, l'efficacité des processus internes de la ville (dont l'achat public dématérialisé) et la sécurité ;
- le *digital manufacturing*, en lien avec l'usine du futur, y compris la mise en œuvre de services via le *cloud*, les robots et la production personnalisée à la demande facilitée par l'impression 3D, la réalité augmentée et la réalité virtuelle, la maintenance prédictive ;
- les transports connectés, les véhicules dotés de capacités d'autonomie et les drones ;
- les services en ligne, avec les besoins exprimés dans le Livre blanc du Cos Management et services, les processus d'innovation avec les plateformes d'intelligence collaborative et les communautés de pratiques ;
- l'accompagnement des jeunes pousses du secteur transformation numérique, qui travaillent sur des métiers très spécifiques (*fintech*, *foodtech…*) ;
- la silver économie, la santé connectée ;
- les industries de confiance et de sécurité (physique ou numérique).

Répondre aux enjeux de société : cohésion sociale, sécurité sociétale, vieillissement… au plan national et européen

Accompagner l'intelligibilité et la réversibilité dans l'économie numérique

La transparence des logiciels et des algorithmes est un enjeu indissociable des données. Cela concerne aussi bien la provenance des données que le contrôle sur ce que réalise un processus logiciel des données : ce qui rentre et ce qui en sort. Plusieurs enjeux pour la normalisation apparaissent à propos de la transparence et de la confiance, qui pourraient se traduire par des axes de recherche et en termes de bonnes pratiques, notamment afin d'associer le processus de décision à la connaissance métier en mettant en œuvre des processus de supervision au sein des organisations.
Technologies et usages du numérique évoluent à un rythme soutenu, ce qui crée des ruptures technologiques importantes à un rythme décennal. Les contenus numériques sont en croissance, naissent et disparaissent au rythme des offres du marché, laissant parfois des chantiers inachevés. La normalisation des modèles de réversibilité des contenus numériques constitue de ce fait un enjeu que la réflexion normative doit s'approprier.

Rôle transverse du Cos

Intégrer le numérique dans les stratégies des autres secteurs

Le Cos ICN doit plus que jamais jouer un rôle transverse d'information, de diffusion et de coordination pour les questions liées au numérique. En fonction de leurs besoins, le Cos est à la disposition des autres secteurs, pour échanger et débattre sur les thèmes utiles pour leurs activités et leur fournir informations et documents sur lesquels s'appuyer. Cela concerne des thématiques pour lesquelles une approche systémique s'avère l'une des méthodes possibles pour approcher le caractère transverse et la complexité du sujet. Exemples : l'e-mobilité et les transports intelligents, l'usine du futur, la ville numérique, les réseaux intelligents, l'e-santé… Les processus de normalisation du numérique demandent une appropriation par les domaines métiers. ●