



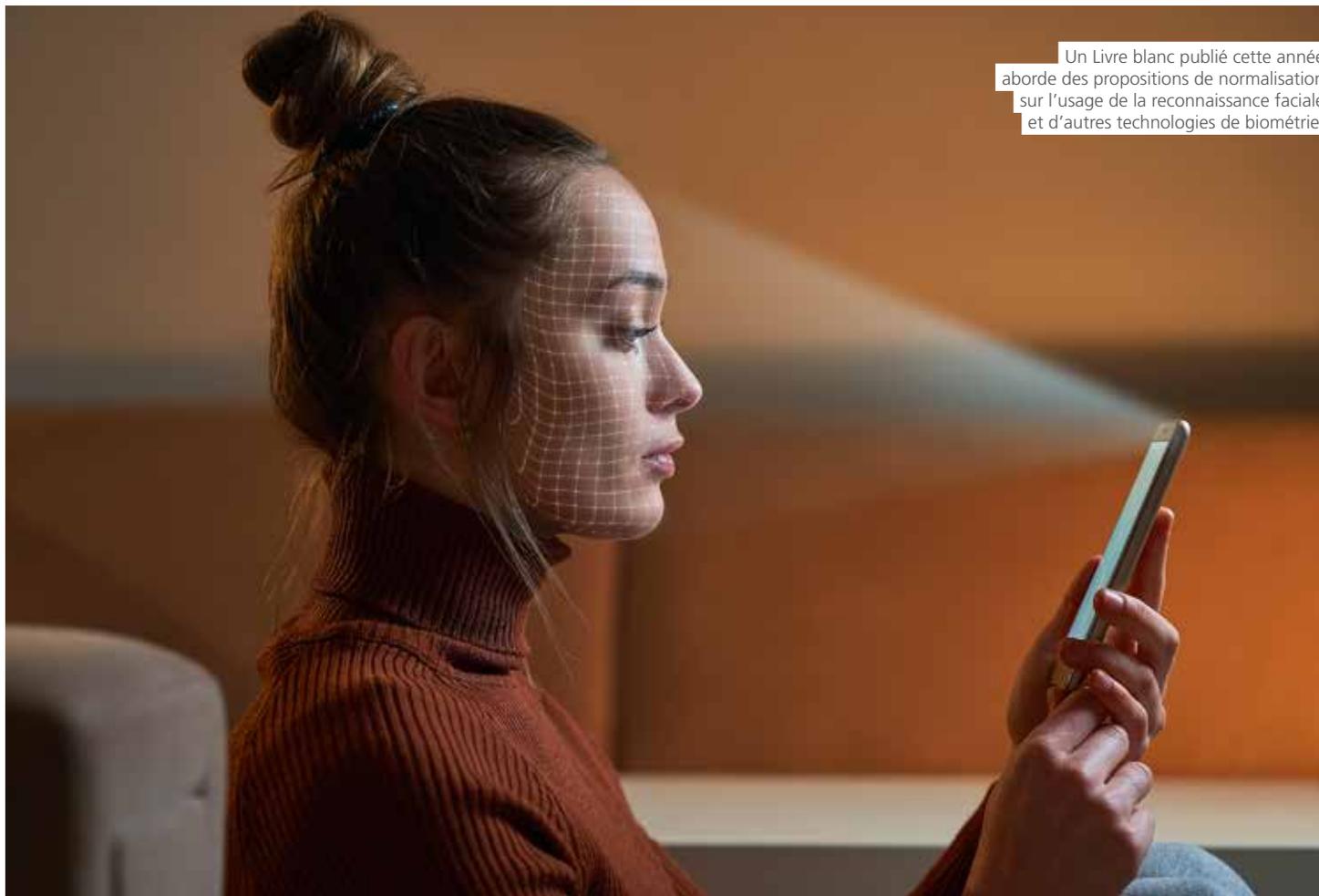
Yves LE QUERREC

Yves LE QUERREC
Président du Cos

Julie LATAWIEC
Rapporteur

Information et communication numérique

Un Livre blanc publié cette année aborde des propositions de normalisation sur l'usage de la reconnaissance faciale et d'autres technologies de biométrie.



Goffkein - AdobeStock

Les normes accompagnent la transformation numérique de l'entreprise et de la société.

Périmètre et contexte

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

Les normes et les documents de référence qui y sont établis sont de nature horizontale et contribuent à apporter des cadres génériques en appui aux travaux dans les secteurs : transport, santé, énergie, ville intelligente, usine du futur, agronomie, etc. Elles facilitent ainsi la transformation numérique de la société, y compris sur des sujets comme l'enseignement et la formation.

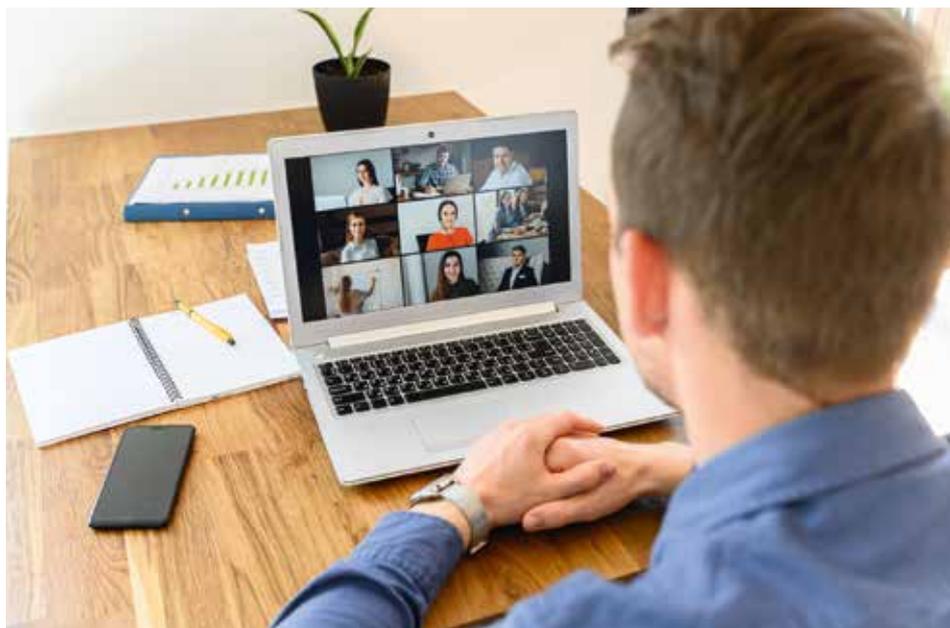
Au-delà des spécificités du monde numérique, le périmètre du Cos porte également sur quelques grands domaines d'applications dans leur globalité : banque, documentation, postal, sécurité du citoyen, commerce électronique et médias.

Les travaux du Cos soutiennent le développement de l'économie sous l'angle de l'écosystème numérique à travers des thématiques transverses que les acteurs du numérique doivent s'approprier. Ces actions et perspectives sont regroupées et présentées ci-après sous la forme de grands domaines étudiés et actualisés en continu par le Cos.

Répondre aux enjeux de la transformation numérique de l'entreprise et de la société

Soutenir par la normalisation la Stratégie française sur l'intelligence artificielle

L'intelligence artificielle (IA) regroupe un ensemble de technologies algorithmiques conduisant à simuler un mécanisme cognitif. Un certain nombre d'initiatives normatives ont été mises en place en France et dans d'autres pays afin d'accompagner le dévelop-



Вадим Пасюк – AdobeStock

pement de l'intelligence artificielle. Il s'agit de sécuriser, fiabiliser, répondre aux enjeux sociétaux, et à terme être capable de certifier les systèmes qui ont recours à l'intelligence artificielle. La normalisation permettra ainsi de coconstruire une IA digne de confiance, responsable, et de lutter contre les biais.

La mise en place d'une stratégie d'accompagnement par la normalisation du développement de l'IA implique de piloter et de contribuer aux travaux normatifs européens et internationaux, la France occupant une position particulière sur l'échiquier des sphères d'influence autour de ces enjeux. Il s'agit également de nouer des alliances pour gagner en efficacité sur les sujets prioritaires.

Enfin, cette approche doit se coordonner avec les besoins des secteurs clés et prioritaires pour la mise en œuvre de ces technologies, notamment ceux ciblés par les priorités du plan d'action stratégique national « Grand Défi ». Afnor accompagnera ainsi en 2021 le « Grand Défi IA », ayant vocation à mettre en œuvre les actions permettant à l'écosystème français de contribuer et d'influencer davantage la constitution des normes et standards européens et internationaux dans le domaine de l'intelligence artificielle, en élaborant les documents normatifs qui permettront d'outiller, à terme, la certification des systèmes à base d'IA.

Développer l'industrie du futur par la numérisation

Le numérique est au cœur des enjeux de l'industrie du futur et de l'innovation. Une coopération d'industriels s'est établie entre plusieurs pays, dont la France, pour développer un cadre commun d'architecture numérique favorisant l'interopérabilité et l'intégration des

technologies. Il est important de se concerter avec nos homologues européens pour adopter les stratégies les plus porteuses afin que la normalisation réponde aux intérêts du tissu industriel français avec ses spécificités.

L'Europe a mis en place une initiative sur la numérisation de l'industrie européenne (Digitising European Industry Initiative [DEI]), qu'il convient de prendre en compte avec discernement afin d'être efficace et d'éviter une dispersion des efforts.

Le Cos est partie prenante du groupe de coordination sur la normalisation de l'industrie du futur. Il contribuera activement à ce programme visant à renforcer l'efficacité des stratégies de développement des filières.

De la transition énergétique à l'économie circulaire

La transition énergétique est une priorité du Cos ICN. Les travaux engagés il y a dix ans ont permis la mise en place de mesures et de bonnes pratiques pour les infrastructures énergie des technologies de l'information et de la communication, qui ont maintenant besoin d'être déployées et promues auprès des acteurs et des pouvoirs publics. Pour autant, le développement exponentiel du numérique s'accompagne d'une explosion de ses besoins énergétiques mondiaux, qui atteignent désormais l'équivalent de la consommation énergétique d'un pays comme la Grande-Bretagne.

Devant l'urgence face à l'impact environnemental et sociétal du numérique, il faudrait étendre la réflexion à l'optimisation du cœur des technologies du numérique, logiciels, matériels et processus, ainsi qu'aux ressources environnementales telles que le CO₂



kerkezz - AdobeStock

La normalisation doit aider à construire une intelligence artificielle digne de confiance et responsable.

Consolider le positionnement français sur la normalisation de la blockchain et les outils de traçabilité

La chaîne de blocs (*blockchain*) est une technologie de rupture apportant potentiellement une réponse à des enjeux d'enregistrement et de traçabilité des transactions de toute nature. Cette technologie s'appuie sur un dispositif distribué de vérification des chaînes associées aux transactions. Il y a aujourd'hui de nombreuses initiatives, et les cas d'usage se multiplient. Ils ne se limitent pas, loin s'en faut, à la monnaie virtuelle.

L'Iso a mis en place en 2017 un comité technique à la demande de l'Australie. L'Europe a également créé un comité technique pour établir des normes complémentaires afin de prendre en compte les spécificités européennes.

Afin de répondre à des enjeux de confiance liés à la fiabilité des données enregistrées dans un système utilisant la technologie *blockchain*, les acteurs français travaillent sur le développement d'une norme nationale visant à apprécier la confiance dans les applications utilisant cette technologie et ainsi diffuser leur usage.

Il s'agira également, pour le Cos, d'évaluer la possibilité d'une déclinaison sectorielle des normes sur la *blockchain* et la traçabilité, pour répondre aux besoins des filières.

Accompagner le déploiement de la 5G

La 5G a pour caractéristiques d'être d'une part une technologie de communication sans fil avec des performances améliorées (débits, temps de latence...) par rapport aux générations précédentes ; d'autre part, elle se veut l'intégration de différents outils, en couvrant le très bas débit des IoT basse consommation jusqu'au très haut débit.

En lien avec les nouveaux services, il faudra mesurer l'impact sur les sujets transversaux, par exemple la télémédecine, la transition écologique et la sécurité globale, puis faire remonter les besoins identifiés vers les instances de normalisation concernées.

Par ailleurs, il est essentiel que la normalisation soit complétée par des cadres de bonnes pratiques pour définir des solutions les plus concrètes possibles venant en appui des besoins sur les territoires.

Soutenir le développement de la fiabilité et de la confiance dans le numérique

Le Cos, en coopération avec les secteurs, aura à développer une réflexion approfondie sur

ou l'eau, donc à toute question présentant un enjeu de société et dont il convient d'apprécier les apports, mais aussi les risques.

Certes, de nombreux travaux coordonnés par le comité visent à accompagner le déploiement de solutions construites sur les technologies numériques qui réduisent les besoins en énergie : mobilité virtuelle, sobriété numérique, dématérialisation, réseaux d'énergie décentralisés. Cependant, les nouvelles technologies, dont la chaîne de blocs (*blockchain*), pour le processus de consensus *proof-of-work* par minage, ou l'intelligence artificielle, pour le processus d'apprentissage profond, demandent urgemment à être optimisées. L'opportunité de leur normalisation peut aider à déployer ces optimisations sans rogner sur l'interopérabilité.

Par ailleurs, les technologies numériques offrent de nouvelles opportunités pour réduire l'impact écologique des activités humaines (par la maîtrise de la consommation, le pilotage de la demande énergétique, etc.). La normalisation doit permettre d'accélérer l'utilisation de ces solutions énergétiques.

Il conviendra de promouvoir une démarche de progrès orientée vers l'économie circulaire avec une déclinaison sectorielle au numérique.

Suivre l'émergence des nouvelles approches technologiques

Se préparer à l'émergence des technologies quantiques dans le numérique

L'ordinateur quantique reposera sur des principes d'architecture et d'algorithmes très différents de ceux mis en œuvre dans les machines actuelles, toutes appliquant les fondements

définis par le mathématicien et physicien John von Neumann. L'avènement du Qbit au sein d'une machine réellement opérationnelle et industrialisée semble proche et aura un impact considérable du fait du gain d'efficacité pour résoudre certains problèmes.

Un risque majeur cependant : toute la sécurité numérique sur laquelle repose l'économie numérique pourrait être remise en cause. Définir ce que sera la sécurité « post-quantique » fait d'ores et déjà l'objet d'une activité de normalisation très importante à l'Iso/IEC/JTC 1 ainsi qu'à l'Etsi.

À l'inverse, les technologies quantiques offrent la perspective de rendre beaucoup plus sûr l'échange de clés de chiffrement sur des réseaux par l'application de propriétés physiques particulières (« syndication »).

La France fait partie des quelques pays qui disposent d'atouts dans ces nouvelles technologies. Les membres du Cos avaient souligné l'importance d'anticiper et de répondre au mieux aux besoins des acteurs français dans un contexte où l'international n'attendra pas. Une consultation sur la création et l'affectation d'un nouveau domaine d'activité sur l'informatique quantique a donc été soumise en mars 2020. Pour faire suite aux résultats de cette consultation, le Cos recommande la constitution d'une instance de travail afin de mettre en chantier deux sujets prioritaires : la méthodologie de comparaison de la performance d'un calcul quantique et l'interface de programmation. L'objectif est de disposer à l'horizon de neuf mois de propositions techniques – type Afnor Spec – françaises, qui permettront d'alimenter à terme de nouvelles propositions de travail européennes ou internationales.

l'apport de la normalisation volontaire pour prendre en compte les préoccupations sociétales (*societal concerns*) et les transformer en avantages compétitifs, plutôt que les percevoir comme une contrainte pour le développement de la société numérique.

Contribuer à la mise en place d'une identité numérique

La construction de l'espace de confiance lié à la digitalisation implique que l'ensemble des solutions existantes et à venir doivent

répondre à des critères d'authentification, de confidentialité et de sécurité des données partagées dont l'identité numérique constitue un élément clé, en accord avec le règlement européen e-IDAS et sa révision.

Cette identité numérique devrait également se décliner pour les objets, en particulier les IoT, et par des besoins normatifs en amont sur, d'une part, l'authenticité des documents qui contribuent à l'enrôlement de l'identité et, sur, d'autre part, les processus de qualification, afin d'en faciliter l'interopérabilité

européenne. Les solutions *blockchain* et la poursuite européenne de la normalisation du cachet électronique visible, issue des travaux du Cos, devraient aussi y contribuer.

L'enjeu de cet effort de normalisation est de parvenir à répondre aux besoins régaliens et aux exigences portées par le marché des services de confiance. Le Cos poursuivra son action visant à cartographier les besoins à couvrir, identifier et évaluer les initiatives afin de proposer des recommandations pour la normalisation.

Renforcer la cybersécurité

Les enjeux de la normalisation sur la cybersécurité portent sur la capacité à mettre en place des infrastructures de confiance de haut niveau en s'appuyant sur, donc en promouvant, le savoir-faire de l'industrie française de sécurité. Ces actions sont menées parallèlement à des actions de sensibilisation de tout le tissu économique à l'intérêt d'une démarche de normalisation par les entreprises. Par son aspect transversal, la cybersécurité a pour vocation d'irriguer l'ensemble de l'écosystème numérique.

Le développement de guides adaptés aux besoins des PME/TPE est aussi un enjeu de souveraineté économique. Ces travaux ont été entamés en particulier par l'Etsi.

Les pouvoirs publics et la réglementation jouent également un rôle majeur dans le domaine de la sécurité. Ce qui se traduit par le soutien de nouvelles réglementations comme, par exemple, celle sur la protection de la vie privée par la normalisation, avec la création de bonnes pratiques immédiatement exploitables.

Pour 2021, le suivi de l'élaboration ou la révision des réglementations en cours (eIDAS, NIS, ePrivacy...) devra faire l'objet d'une attention particulière.

Un autre enjeu existe dans la gouvernance avec le Cybersecurity Act. Ce règlement européen renforce les compétences de l'agence européenne European Union Agency for Cybersecurity (Enisa) et concerne notamment la mise en place de schémas de certification pour tous les produits, solutions et services. Au niveau opérationnel, il est essentiel que ces schémas de certification s'appuient sur des normes. Le Cos ICN reste vigilant dans le suivi du développement, notamment sur la 5G et les IoT, de ces standards, tout comme les travaux du Stakeholder Cybersecurity Coordination Group (SCCG), dans lequel les organismes de normalisation internationaux sont représentés (Cen, Cenelec, Etsi).

NORMES ET DOCUMENTS NORMATIFS IMPORTANTS PUBLIÉS EN 2020

NF Iso 3297	Information et documentation – numéro international normalisé des publications en série (ISSN)
Iso 19161-1	Références géodésiques – partie 1 : système international de référence terrestre (ITRS)
Iso/IEC 29184	Technologie de l'information – avis de confidentialité en ligne et consentement
EN Iso/IEC 27019	Technologies de l'information – techniques de sécurité – mesures de sécurité de l'information pour l'industrie des opérateurs de l'énergie
EN 303645	Cyber – cybersécurité pour l'Internet des objets grand public : exigences de base (V2.1.1)
Iso/IEC 27006:2015/Amd 1:2020	Technologies de l'information – techniques de sécurité – exigences pour les organismes procédant à l'audit et à la certification des systèmes de management de la sécurité de l'information – amendement 1
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 27009	Technologies de l'information – techniques de sécurité – application de l'Iso/IEC 27001 à un secteur spécifique – exigences
NF Z 42-013	Archivage électronique – spécifications relatives à la conception et à l'exploitation de systèmes informatiques en vue d'assurer la conservation et l'intégrité des documents stockés dans ces systèmes
Iso/TR 23244	Blockchain et technologies de registre distribué – considérations de protection de la vie privée et de protection de l'information personnellement identifiables
Série Iso 3166	Codes pour la représentation des noms de pays et de leurs subdivisions Partie 1 : codes de pays Partie 2 : code pour les subdivisions de pays Partie 3 : code pour les noms de pays antérieurement utilisés

fofomek - AdobeStock



Les cas d'usage de la *blockchain* se multiplient, bien au-delà de la monnaie virtuelle. Iso et Cen ont mis en place des comités techniques.

champ d'un contrôle nécessaire sur la partie du cyberspace qui le concerne, dont il est devenu dépendant pour son fonctionnement avec sa population, qui s'est construite sans lui, et qui affecte sa souveraineté et son autonomie stratégique.

Assurer la confiance dans les API par la certification

La problématique de certification des interfaces de programmation applicatives (Application Programming Interface, API) devient un sujet de préoccupation pour les concepteurs et utilisateurs de ces microservices. Identité numérique (OSIA, FranceConnect...), services financiers (DSP 2, *open banking*, *open data*)... l'ensemble des services se développent autour des API. Bien structurée et intégrée dans les architectures logicielles (Representation State Transfer, REST-OpenAPI Swagger, RESTful API Modeling Language RAML ; GraphQL...), la partie implémentation des API reste encore démunie de référentiels pour leur certification.

Le Cos ICN, qui a initié une réflexion sur ce sujet et où est déjà identifiée la séparation entre le modèle logique et l'implémentation métier, tant côté serveur que côté client, poursuivra en 2021 ce travail sous forme d'une

Enfin, le Cos restera attentif à la cohérence du dispositif de normalisation, y compris sur les cas d'usage, en assurant la liaison, aux niveaux européen et international, avec les travaux des comités Iso/IEC/JTC 1/SC 27, Cen/Cenelec/JTC 13 et Etsi/TC Cyber, qui jouent un rôle central dans le développement des normes.

Répondre aux enjeux liés à la reconnaissance faciale

Le Cos a constitué en 2020 un groupe de travail afin de rédiger un Livre blanc relatif à des propositions de normalisation sur l'usage de la reconnaissance faciale et plus largement les technologies de biométrie qui peuvent être associées (détection du vivant, émotions...). L'échéance de ce projet, prévue en 2021, permettra de promouvoir ces ouvertures à l'échelon national, européen et/ou international. Les travaux prennent en compte la dimension éthique, la robustesse et la certification propre aux concepts déjà développés dans l'intelligence artificielle, mais aussi la dimension sociétale et juridique liée à l'utilisation de cette technologie.

Développer le concept de territorialité numérique

Le Cos est en appui de l'étude engagée par la commission de normalisation Intelligence artificielle (CN IA) et la commission de

normalisation Cybersécurité (CN SSI), qui ont décidé d'unir leurs forces et leur savoir-faire pour mener à bien la présentation d'un concept exploratoire de territorialité numérique.

Il existe une notion de territoire physique. Cette étude a pour objectif de projeter cette notion au numérique, notamment en vue d'explicitier comment le champ de l'intervention et de la responsabilité régaliennne, de la politique et des doctrines, voire de la souveraineté pourrait être transposé dans le cyberspace.

Définir et modéliser le territoire numérique devrait permettre à un État de mieux élaborer et expliquer sa stratégie et de légitimer le



Le développement exponentiel du numérique et ses besoins énergétiques soulèvent des questions environnementales et sociétales.

Framesstock - AdobeStock

plateforme collaborative et fournira un premier document de recommandations du type bonnes pratiques.

Confirmer la place de la normalisation des interfaces utilisateurs

Il est primordial, dans le cadre d'une appropriation et de la construction de la confiance dans la transition numérique de notre société, de donner une place prépondérante aux travaux portant sur l'interface utilisateur développés par le JTC 1/SC 35. L'année 2020 a vu une montée en charge importante de la production des services numériques, qui doit prendre en charge les besoins d'accessibilité et les autres besoins spécifiques comme l'adaptabilité culturelle et linguistique. Le Cos veillera à l'implication de cette partie dans tous les travaux de normalisation.

Encourager les initiatives de portages des normes françaises à l'international

Soutenir le process de lancement d'un nouveau comité technique au Cen sur l'archivage électronique

Les travaux français, en particulier avec la révision récente de la norme NF Z 42-013 publiée fin 2020, ont été proposés à la normalisation européenne (Cen/BT WG 6) dans le cadre de la création d'un nouveau comité technique, ce domaine n'étant pas encore couvert au sein du Cen. Le Cos ICN est en appui de cette initiative pour la promotion des travaux français de normalisation, qui dans ce domaine sont leader, et parce qu'elle arrive à point nommé dans le cadre de la révision du règlement eIDAS et l'intégration possible du concept de système d'archivage électronique (SAE) comme service de confiance. Partiellement portés dans le cadre de l'Iso au TC 171, les travaux devraient trouver, au Cen, une nouvelle dimension avec les autres travaux réglementaires comme eIDAS, le RGPD et les travaux sur le *cloud computing*.

Appuyer la création d'une norme internationale sur le cachet électronique visible

La publication du nouveau document XP Z 42-105 en 2020 s'est accompagnée d'une démarche de portage des travaux sur le cachet électronique visible à l'international.

Suivis par le Cos ICN, qui a approuvé cette initiative, les travaux viennent d'être poussés par la commission Afnor en charge du sujet à l'Iso/TC 292/WG 4 dans le nouveau projet Iso/AWI 22385 Sécurité et résilience – authenticité, intégrité et confiance pour les produits

et les documents – lignes directrices pour l'établissement d'un cadre d'orientation et d'interopérabilité. Le Cos appuiera ces travaux, qui devaient également être portés au Cen pour valoriser la compatibilité eIDAS de l'infrastructure. ●

NORMES ET DOCUMENTS NORMATIFS IMPORTANTS PRÉVUS EN 2021

EN Iso/IEC 27701	Techniques de sécurité – extension d'Iso/IEC 27001 et Iso/IEC 27002 au management de la protection de la vie privée – exigences et lignes directrices
Iso/IEC 20008-2	Technologies de l'information – techniques de sécurité – signatures numériques anonymes – partie 2 : mécanismes utilisant une clé publique de groupe
Iso/IEC 27022	Orientations pour les processus du système de gestion de la sécurité de l'information
Série Iso/IEC 15408	Technologies de l'information – techniques de sécurité – critères d'évaluation pour la sécurité TI Partie 1 : introduction et modèle général Partie 2 : exigences fonctionnelles de sécurité Partie 3 : exigences d'assurance de sécurité Partie 4 : cadre de spécification des méthodes et activités d'évaluation Partie 5 : paquets prédéfinis d'exigences de sécurité
Iso/IEC 18045	Technologies de l'information – techniques de sécurité – méthodologie pour l'évaluation de sécurité TI
Iso/IEC 20897-1	Sécurité de l'information, cybersécurité et protection de la vie privée – fonctions physiquement non clonables – partie 1 : exigences de sécurité
Iso/IEC 20897-2	Sécurité de l'information, cybersécurité et protection de la vie privée – exigences de sécurité et méthodes de test pour les fonctions physiquement non clonables pour générer des paramètres de sécurité non stockés – partie 2 : méthodes d'essai et d'évaluation
Iso/IEC 27002	Technologies de l'information – techniques de sécurité – code de bonne pratique pour le management de la sécurité de l'information
Iso/IEC 30134-6	Technologie de l'information – centres de données – indicateurs de performance clés – partie 6 : facteur de réutilisation de l'énergie (ERF)
Iso 690	Information et documentation – principes directeurs pour la rédaction des références bibliographiques et des citations des ressources d'information