2026

PANORAMA DES NORMES DE SÉCURITÉ-SÛRETÉ

ACN

Alliance pour la confiance numérique

Rapport de la commission NORSEC du CSF “Industries de sécurité” coordonné par l'ACN

Table des matières

Avant-propos

Un document par nature évolutif

La sécurité constitue un enjeu majeur, qu'il s'agisse de la protection des personnes, des infrastructures, des données ou de l'information. Afin de répondre à cet enjeu, les exigences règlementaires évoluent dans le temps dans l'objectif à la fois de s'assurer que toutes les parties prenantes se comprennent sans délai et de faire face aux menaces en perpétuelle mutation. Il est donc nécessaire de disposer d'une vision claire et structurée des normes applicables en matière de sécurité.

Dans ce document, le terme « normalisation » est entendu comme désignant le processus structuré d'élaboration, de publication et d'application de normes techniques volontaires, élaborées par consensus pour standardiser des produits, services, méthodes ou processus afin d'assurer compatibilité, qualité, sécurité et efficacité. Ces processus permettent d'élaborer des documents de référence (« normes ») ayant un caractère volontaire, consensuel et technique. Le terme « normes » tel qu'utilisé dans ce document se distingue donc de l'acception beaucoup plus large, souvent utilisée en langage courant, intégrant dans la notion de « norme » les normes juridiques (dispositions législatives ou réglementaires), sociales, etc.

Le présent document a été rédigé par l'ACN dans le cadre de la commission NORSEC (NORmalisation en SECurité) du Comité Stratégique de Filière des Industries de Sécurité (CSF IS). Ce document a pour objectif de cartographier les normes essentielles pour la sécurité[1]. De fait, il identifie les principaux comités de normalisation et les normes stratégiques pour ce domaine.

Ainsi, s'il dresse un panorama dense sans pour autant avoir vocation à être exhaustif, il est important de rappeler que ce document ne peut être un document figé, **la normalisation étant dynamique et évolutive par nature**, dans la mesure où les besoins se transforment au gré des menaces, comme des évolutions technologiques. En effet, la **révision régulière des normes techniques garantit l'alignement avec l'évolution de l'état de l'art**, intégrant les avancées scientifiques, et technologiques.

[1] Le terme de « sécurité » inclut les normes de sécurité numérique et les normes de sécurité physique et industrielle (incendie, équipements de protection, sûreté des installations etc.).

Dans quel contexte s'inscrit le document ? Quel est le besoin actuel ?

Le domaine de la normalisation est un domaine complexe et soumis à de nombreux préjugés. La normalisation est souvent perçue - à tort - comme trop coûteuse, voire comme un frein à l'innovation, en dépit des nombreux aspects stratégiques souvent occultés. Les normes renforcent la sécurité, la résilience, et aident les entreprises à optimiser leurs processus, réduire les coûts et accéder à de nouveaux marchés. La France se place au cinquième rang à l'ISO au nombre de structures techniques gérées. Ses industriels sont ainsi aux avant-postes sur de nombreux domaines stratégiques tels que l'informatique industrielle, la biométrie, l'énergie, l'eau, l'environnement, la sécurité – résilience ou encore la cybersécurité. Cependant, la multiplicité des travaux et des acteurs en matière de normalisation rend quelquefois difficile l'identification des risques et opportunités dans ce domaine.

5ÈME

C'est le classement de la France à l'ISO au nombre de structures techniques gérées.

A qui s'adresse le document ?

Ce support s'adresse donc aux utilisateurs quotidiens des normes, aux pouvoirs publics et aux acteurs économiques. Il entend :

- Promouvoir la normalisation pour ses caractéristiques et atouts stratégiques et appuyer la mise en conformité en renforçant la culture de sécurité.

- Soutenir la résilience collective, dans l'optique de créer un environnement plus sûr et plus résilient.

- Faire comprendre les enjeux propres à la normalisation afin de faciliter la compréhension, l'accessibilité et l'appropriation par les différents acteurs concernés, mais aussi par le grand public.

- Cartographier les normes via une lecture transversale : il s'agit d'établir la liste la plus complète possible des différentes normes techniques existantes (aux niveaux internationaux, nationaux et sectoriels) et des comités de normalisation.

Au-delà de ces objectifs, il convient d'illustrer concrètement les bénéfices tangibles de la normalisation et son rôle structurant dans la résilience collective.

20 % à 40%

C'est la contribution estimée de la normalisation à la croissance de la productivité dans les économies industrialisées.

Les normes ne sont pas de simples documents techniques : elles constituent des outils de compétitivité, de confiance et de souveraineté. Leur adoption permet d'améliorer la qualité et la sécurité des produits, de réduire les coûts liés à la non-conformité, et d'accélérer la mise sur le marché des innovations. Selon plusieurs études ISO, CEN-CENELEC et AFNOR[2], la normalisation contribue entre 20% et 40% de la croissance de la productivité dans les économies industrialisées. Les entreprises engagées dans ces démarches affichent en moyenne une productivité supérieure d'environ 20 % et une réduction de 10 à 25 % des coûts de non-qualité, illustrant l'impact direct de la normalisation sur la compétitivité et la maîtrise des risques. Sur le plan collectif, les normes soutiennent la résilience nationale et européenne en offrant un langage commun de la sécurité. Leur mise en œuvre coordonnée entre acteurs publics, opérateurs d'importance vitale, PME et organismes d'évaluation favorise une approche cohérente de la prévention, de la réponse et de la continuité d'activité face aux crises technologiques, naturelles ou cyber.

En somme, promouvoir la normalisation revient à anticiper les risques plutôt qu'à les subir, à renforcer la confiance dans les technologies et à asseoir la souveraineté économique et technologique de la France et de l'Europe dans un environnement mondialisé.

Le présent document a été conçu et structuré pour rendre plus lisible le panorama actuel de la normalisation et pour aider les acteurs de la filière à s'approprier cet outil stratégique. Tout d'abord, l'introduction entend poser les bases de la normalisation. Puis une première partie vient analyser en profondeur les enjeux propres à la normalisation. Enfin, l'ultime partie veut dresser une liste la plus exhaustive possible des normes et des comités de normalisation existants.

[2] AFNOR / BIPE, *L'impact économique de la normalisation – Évaluation macroéconomique et microéconomique en France*, 2009, réédité 2016, https://normalisation.afnor.org/wp-content/uploads/2016/06/Etude-ImpactEcoNorm-GB2009.pdf.
CEN & CENELEC, *Standardization boosts productivity and trade: A macroeconomic study*, Centre for Economics and Business Research (Cebr), 2023, https://www.cencenelec.eu/news-events/news/2023/brief-news/standardization-boosts-productivity-and-trade-a-macroeconomic-study/.
ISO, *Economic impact of standards – Methodological guidance*, ISO Publication, 2021,https://www.iso.org/files/live/sites/isoorg/files/store/en/PUB100465.pdf.

Introduction : précisions terminologiques

L'article 2 du règlement (UE) N°1025/2012 relatif à la normalisation européenne donne la définition suivante : on entend par « **norme** », une spécification technique, approuvée par un organisme reconnu de normalisation, pour application répétée et continue, dont le respect n'est pas obligatoire et qui relève de l'une des catégories suivantes :

- « Norme internationale » ; une norme adoptée par un organisme international de normalisation.
- « Norme européenne » ; une norme adoptée par une organisation européenne de normalisation.
- « Norme harmonisée » ; une norme européenne adoptée sur la base d'une demande formulée par la Commission pour l'application de la législation d'harmonisation de l'Union.
- « Norme nationale » ; une norme adoptée par un organisme national de normalisation.

Les **normes** peuvent émaner d'initiatives variées. Elles sont élaborées avec des experts issus de divers secteurs à travers le monde présents au sein d'organismes spécialisés, le plus souvent étatiques, comme l'Afnor, agréés au niveau régional (comme le CEN, CENELEC ou le ETSI), ou encore issues d'un traité international (comme ISO), voire des organisations créées par les professionnels d'un secteur d'activité donné. Mais leur élaboration repose souvent sur une coopération technique internationale.

Par extension, la **normalisation** désigne donc le processus d'attribution d'une norme. En vertu du décret N°2009-697 du 16 juin 2009, la normalisation est vue comme « une activité d'intérêt général qui a pour objet de fournir des documents de référence élaborés de manière consensuelle par toutes les parties intéressées, portant sur des règles, des caractéristiques, des recommandations ou des exemples de bonnes pratiques, relatives à des produits, à de services, à des

méthodes, à des processus ou à des organisations »[3]. Elle est de nature volontaire, largement soutenue par les milieux industriels qui la financent en grande partie. La normalisation est utilisée dans des domaines majeurs de la vie économique : énergie, transport, matériaux, BTP, biens d'équipement, biens de consommation, management et services, santé, agroalimentaire, environnement, technologies de l'information et de la communication, etc.[4].

La confusion entre les termes « norme » (en anglais standard) et « standard » (en anglais convention), est fréquente bien que chacun ait une signification précise et renvoie à un périmètre précis. Le **standard**, lui, renvoie à une habitude ou une convention largement adoptée pour une communauté précise, sans pour autant qu'il y ait un processus institutionnalisé, d'obligation de transparence ou de consensus.

Le point de vue de Roland Atoui,

Président de la commission NORSEC, Fondateur et Directeur Red Alert Labs

Du point de vue d'un organisme d'évaluation et de certification, la valeur d'une norme ne se mesure pas seulement à sa qualité technique, mais à sa capacité à produire des exigences claires, testables et auditables, avec des critères d'acceptation non ambigus. L'arrivée du Cyber Resilience Act renforce cette exigence : il faut pouvoir démontrer la conformité de manière robuste, comparable et reproductible, y compris sur des sujets complexes comme la gestion des vulnérabilités, la chaîne d'approvisionnement ou la mise à jour de sécurité. Une cartographie des normes essentielles permet de réduire l'incertitude, d'aligner les pratiques des évaluateurs, et de sécuriser l'interprétation entre industriels, autorités et CAB. C'est aussi un levier concret pour accélérer les parcours de conformité, éviter les divergences d'audit, et renforcer la crédibilité des certifications sur le marché européen.

[3] DGE, La normalisation et l'accréditation, Publié le 11 octobre 2024, mis à jour le 29 janvier 2026, https://www.entreprises.gouv.fr/espace-entreprises/s-informer-sur-la-reglementation/la-normalisation-et-laccreditation.
[4] Ibid.

I. La normalisation : intérêts stratégiques, défis, dynamiques structurantes

1. La normalisation, levier stratégique d'innovation, de compétitivité et de durabilité

Ainsi, à la croisée des défis actuels de développement économique, d'innovation et de développement durable, la normalisation est un levier stratégique majeur **d'innovation, de compétitivité et de durabilité**.

Tout d'abord, la normalisation permet d'implanter un cadre harmonisé tout en contribuant à un environnement sécurisé. Les normes occupent une place centrale dans la construction du marché unique européen et dans l'intégration des échanges au sein de l'économie mondiale. Aujourd'hui, la majorité de ces normes est élaborée au niveau européen et international, assurant une compatibilité accrue des produits, services et procédés sur les marchés mondiaux soumis à la mondialisation[5]. Cette interopérabilité réduit de fait les obstacles techniques au commerce, en accord avec les principes défendus par l'OMC, et contribue à fluidifier les échanges commerciaux. Ainsi, la Commission européenne produit un grand nombre de règlements et directives dans le domaine de la sécurité qui nécessitent le développement d'un corpus de normes pour soutenir cet effort règlementaire. Pour ce faire, la Commission émet des SR (*standardisation request*) soumises aux organismes européens de standardisation. En somme, gages de fiabilité et de compatibilité, **les normes favorisent la durabilité en fournissant un cadre normatif stable et universel**.

Mais ce langage technique commun permet aux chercheurs, ingénieurs et industriels de collaborer efficacement au-delà des frontières technologiques et géographiques, ce qui soutient un cycle en faveur de **l'innovation**. Les normes accélèrent la diffusion des technologies, en rendant possible la délocalisation des productions. Plus encore, pour les acteurs économiques, la normalisation dans sa nature fournit un espace diffusant l'innovation. La participation aux comités de normalisation est un moyen d'échanger avec des spécialistes et experts ce qui favorise la coopération, créatrice de nouvelles solutions technologiques.

[5] Ibid.

L'exemple du secteur du sans-fil illustre comment les normes ont catalysé une **croissance rapide et structurée de l'industrie**[6].

Figure 1 : La normalisation : à quoi ça sert ?

2. La normalisation, miroir des intérêts économiques et politiques et des rivalités géopolitiques

Si les normes sont toujours volontaires et reposent sur le consensus international d'experts de nombreux pays, leur adoption réelle par les entités politiques et économiques est large. En effet, les normes internationales sont souvent adoptées pour devenir des normes nationales ou régionales. Par exemple, près de 80 % des normes électriques et électroniques européennes sont en fait des normes internationales de la CEI[7]. Ainsi, en étant à l'initiative d'une norme internationale, dont l'application est purement volontaire, les Etats ou industries peuvent

[6] Securing Global Standards for Innovation and Growth, 2022, https://www.csis.org/analysis/securing-global-standards-innovation-and-growth.

[7] International Electrotechnical Commission, 2026, https://www.iec.ch/understanding-standards.

influencer les réglementations dans plusieurs pays et façonner le monde avec des normes conformes à leurs intérêts.

L'adoption d'un ensemble de normes par rapport à un autre peut conférer des avantages à des entreprises et à des économies nationales particulières. En effet, les processus normatifs sont façonnés par les rapports de force économiques et politiques dans la mesure où les acteurs (publics comme privés) y voient un levier stratégique.

Ainsi, la normalisation est un excellent révélateur des objectifs stratégiques des différents pays, mais aussi des grands industriels multinationaux (Amazon, Meta, Huawei, Alibaba, Tencent, etc.). Au niveau européen, des entreprises nord-américaines comme Microsoft, IBM, Amazon, Apple, ou Google sont très présentes dans des comités comme le JTC21 (normes IA) et manquent parfois de transparence sur leurs véritables intérêts[8]. En effet, les intérêts motivant une occupation accrue des instances de normalisation sont nombreux. Ils comprennent notamment l'acquisition d'avantages concurrentiels, qui se fait en structurant les pratiques et en harmonisant les référentiels techniques.

Toutefois, la concurrence entre l'Union Européenne (UE) et la Chine pour fixer des normes mondiales est peut-être l'exemple le plus significatif de ce rapport de force. Cette conflictualité renvoie directement à un phénomène appelé « effet de Bruxelles », que la Chine tente de contrebalancer via son « effet de Pékin » [9]. L'effet de Bruxelles désigne la capacité de l'Union européenne à façonner l'espace règlementaire via sa puissance normative. L'UE constitue un marché de taille, mais règlementé par des normes, auquel les entreprises doivent se conformer si elles souhaitent s'y implanter. En se soumettant à ces obligations normatives du marché européen, les entreprises étendent souvent ces règles à l'ensemble de leurs produits, services ou infrastructures, y compris ceux sur des marchés mondiaux aux normes moins strictes. Cela s'explique par la volonté d'éviter les coûts liés au respect de plusieurs régimes règlementaires. Ainsi, sans avoir recours à la coercition, à l'influence ou à la coopération, l'UE parvient à diffuser ses normes du marché européen au marché mondial grâce aux entreprises qui servent alors d'intermédiaires comme l'illustrent les domaines suivants : protection des données, définition du discours haineux sur les plateformes, etc. Le pouvoir règlementaire chinois est en expansion, bien que relativement faible en comparaison. Mais c'est via son pouvoir économique, et plus particulièrement son

[8] Corporate Europe Observatory, 2025,https://corporateeurope.org/en/2025/01/bias-baked.
[9] Financial Times, 2019,https://www.ft.com/content/0c91b884-92bb-11e9-aea1-2b1d33ac3271.

influence au sein de l'économie numérique, que la Chine diffuse ses normes technologiques dans le processus. Si l'effet de Bruxelles n'est pas un outil géopolitique à proprement parler, il s'inscrit comme un élément constitutif de la compétition normative entre l'UE et la Chine.

Au-delà d'intérêts privés, la normalisation joue un rôle dans la diffusion de certains modèles de société[10]. Dans l'UIT, la Chine a soumis **des projets de normes techniques** pour les systèmes de surveillance intelligente. Mais ce type de norme légitime non seulement son **modèle de société** caractérisé par la centralisation, la surveillance, et le contrôle des données, mais l'institutionnalise également. Ainsi, la surveillance par caméra n'est plus un choix politique mais une **bonne pratique technique internationale**. De plus, les pays qui adoptent ces normes (souvent dans le cadre des « Nouvelles routes de la soie numériques ») ont souvent recours à des technologies chinoises dans la mesure où les entreprises chinoises, pionnières en la matière, disposent des systèmes conformes. En contrepartie, via ses normes européennes en matière de protection des données (RGPD), l'Union européenne diffuse elle aussi son modèle de société libéral. Ce modèle repose sur des principes de **protection de la vie privée, de consentement, de transparence, de droit à l'oubli, et de décentralisation de la gestion des données** et inspire des lois de protection des données au **Brésil, au Nigeria ou au Kenya**.

3. Etude de cas : la stratégie normative chinoise au service de la puissance technologique

Alors que les standards techniques occidentaux dominent le marché mondial, assurant l'interopérabilité des produits, **la Chine ambitionne de dépasser la puissance normative occidentale depuis plusieurs années**. Conscients de l'importance des normes comme levier de puissance, les fleurons chinois investissent massivement les instances de normalisation, soutenus par la mise en place de politiques et de financements étatiques[11].

[10] The Diplomat, The Brussels Effect and China: Shaping Tech Standards, 2021,https://thediplomat.com/2021/01/the-brussels-effect-and-china-shaping-tech-standards.

[11] The Wall Street journal, 2021, https://www.wsj.com/world/china/from-lightbulbs-to-5g-china-battles-west-for-control-of-vital-technology-standards-11612722698.

L'effort de montée en puissance au niveau normatif impulsé par la Chine accompagne des **ambitions économiques et technologiques claires**. Il s'agit de faire en sorte que ses standards deviennent globaux, ce qui incite les autres pays à adopter son écosystème technologique (Huawei, ZTE, Xiaomi, SenseTime, etc.). Via les instances de normalisation, Pékin souhaite obtenir un avantage concurrentiel pour les entreprises chinoises et privilégier les entreprises nationales telles que Huawei par rapport à ses concurrents mondiaux. En implantant des normes qui correspondent aux technologies chinoises, la Chine peut augmenter ses exportations.

Pour ce faire, les grands fleurons de l'industrie technologique chinoise -souvent affiliés au Parti Communiste Chinois (PCC) - **investissent massivement les organismes de normalisation internationaux**, via leur présence dans les groupes de normalisation nationaux des principaux pays. Globalement, les délégations chinoises espèrent obtenir environ deux fois plus de postes de secrétaire qu'il y a dix ans[12]. Parmi ces entités, l'Union internationale des télécommunications (UIT), ou encore l'Organisation internationale de normalisation (ISO) voient la présence chinoise s'accroître.

L'UIT, basée à Genève, définit les standards mondiaux en matière de télécommunications. Un responsable chinois dirige l'UIT et des représentants de Pékin siègent dans plusieurs comités stratégiques, avec des postes de rapporteurs notamment. Ces postes leur permettent d'exercer une influence sur les propositions, les débats et les priorités comme en témoigne l'introduction de 2 000 nouvelles propositions de normes aux groupes d'étude de l'UIT sur des sujets tels que la 5G, la cybersécurité et l'intelligence artificielle portée par Huawei[13].

Parallèlement, l'ISO est aussi le théâtre d'une présence croissante de la Chine. Pékin a tenté d'avoir recours à l'ISO afin de propager ses normes domestiques à une échelle internationale. Avec un cadre domestique consolidé grâce à des normes élaborées au sein de l'institut chinois de normalisation de l'électronique, la Chine a tenté de pousser ses normes au sein du comité de l'ISO sur l'IA, via des livres blancs. Cette démarche illustre une volonté plus large de faire accepter ses modèles technologiques comme références universelles, réduisant ainsi la dépendance aux normes occidentales.

[12] The Wall Street Journal, From Lightbulbs to 5G, 2021https://www.wsj.com/world/china/from-lightbulbs-to-5g-china-battles-west-for-control-of-vital-technology-standards-11612722698.
[13] CSIS, Securing Global Standards for Innovation and Growth, 2021, https://www.csis.org/analysis/securing-global-standards-innovation-and-growth.

La stratégie de la Chine pour devenir un arbitre incontournable des standards mondiaux se caractérise par un traitement ambivalent et asymétrique : la méthode du « ***carrot and stick*** » (**carotte et bâton**). À l'échelle internationale, elle use de la « carotte » : elle cherche à obtenir le soutien de certaines entreprises étrangères dans les votes techniques en proposant en contrepartie des avantages commerciaux, voire des transactions discrètes. En revanche, sur le plan intérieur, Pékin privilégie le « bâton » : les acteurs étrangers sont souvent écartés des processus de normalisation nationaux. Cependant, si l'influence et la puissance chinoises croissent, il existe des freins indéniables qui limitent le succès des normes poussées. Un rapport de l'Institut suédois des affaires internationales relativise leur portée : la majorité des propositions chinoises soumises aux organismes internationaux, comme l'ISO, sont rejetées dès les premières étapes, souvent pour des questions techniques (faible qualité, pertinence relative) et de leur manque de **crédibilité** auprès de la communauté mondiale (défiance et résistance)[14].

[14] Financial Times, Technology: how the US, EU and China compete to set industry standards, 2019,https://www.ft.com/content/0c91b884-92bb-11e9-aea1-2b1d33ac3271.

II. Les comités de normalisation retenus : des comités complémentaires, actifs à différentes échelles

Qu'est-ce qu'un comité de normalisation ?

Les comités de normalisation désignent les organismes composés d'experts de différents pays et secteurs, en charge de la normalisation, soit du processus de définition, d'élaboration et de publication des normes.

Ces comités s'articulent à plusieurs échelles : on retrouve des comités internationaux, européens, nationaux et techniques. Malgré cette pluralité, et des prérogatives particulières, les comités coopèrent afin qu'il n'y ait pas de contradictions dans les normes.

Quels principes régissent les organismes de normalisation ?

Les organismes de normalisation s'engagent à respecter les principes reconnus par l'Organisation mondiale du commerce (OMC)[15] :

- **Transparence** : accès aux informations facilité, délais mis en place et possibilité de formuler des observations.
- **Ouverture** : participation sans discrimination de toutes les parties prenantes.
- **Impartialité** : élaboration des normes sans favoriser d'intérêts particuliers.
- **Consensus** : recherche d'un accord général prenant en compte tous les avis, bien que cela n'implique pas pour autant l'unanimité.
- **Efficacité** : définition des normes basée sur l'aptitude à l'usage.
- **Pertinence** : révision régulière (tous les 5 ans) pour s'aligner avec les évolutions.
- **Cohérence** : coordination à plusieurs niveaux (comprenant les échelles nationales et internationales).

[15] Ministère de l'économie de l'industrie et du numérique, 2016, https://www.entreprises.gouv.fr/files/files/Publications/2016/guides/2016-guide-pratique-du-bon-usage-de-la-normalisation-dans-la-reglementation.pdf.

Quels sont les enjeux propres à ces organisations ?

Comprendre qui crée les normes permet d'identifier les enjeux, les dynamiques d'influence et les canaux par lesquels les entreprises et États peuvent intervenir via la normalisation. En d'autres termes, ces comités façonnent les conditions dans lesquelles s'applique la sécurité à l'ensemble du monde, ce qui constitue un levier d'influence considérable. Il est donc crucial de déterminer dans quels comités, certains acteurs économiques et politiques s'insèrent afin de mieux appréhender les dynamiques et rivalités géostratégiques.

1. Les comités internationaux

Parmi les comités de normalisation, on retrouve des comités internationaux. Ils sont tous chargés de l'établissement des normes applicables à l'échelle internationale, avec des prérogatives néanmoins distinctes.

Toutefois, ces comités n'ont pas de pouvoir législatif contraignant. Les normes introduites par ces comités fonctionnent comme des références fixant des exigences techniques, des critères de qualité, et de sécurité, non-contraignantes. Ainsi, leur application dépend de la volonté des Etats. Si leur application est volontaire, elle est souvent incontournable, car l'interopérabilité est un critère majeur dans les échanges commerciaux. C'est ainsi que les états adoptent ces normes dans leur réglementation nationale.

Du fait d'une longue histoire, **il existe trois grands comités internationaux de normalisation : l'ISO, l'UIT et l'IEC**. Comme on le verra plus loin, l'ISO et l'IEC travaillent ensemble sur un certain nombre de sujets, au travers de comités communs (JTC – *Joint Technical Comittees*). Par ailleurs, des analyses complémentaires portant sur l'IETF (*Internet Engineering Task Force*) et l'IUT seront développées dans une version ultérieure de ce document.

a) L'ISO (*International Organization for Standardization*)

Créée en 1947, l'ISO (qui signifie *International Organization for Standardization*), est l'un des trois organismes internationaux dépendant de l'ONU et basés à Genève[16].

[16] ISO, https://www.iso.org/fr/a-propos.

Composée d'experts, sa mission principale est **d'élaborer des normes internationales** sur base de consensus. Son objectif est de garantir la cohérence, la qualité et la compatibilité à l'échelle mondiale couvrant un très grand nombre de domaines : industrie, environnement, sécurité, technologies, santé, etc. Grâce à ses comités spécialisés, il élabore des normes de référence qui couvrent aussi bien la **cybersécurité**, la **vie privée**, la **gestion de crise**, que des sujets émergents comme **l'intelligence artificielle**, **l'Internet des objets** ou **la blockchain**.

Son financement trouve son origine dans les cotisations de ses membres et la vente de ses normes publiées[17]. Parmi les nombreux comités et sous-comités de l'ISO, deux jouent un rôle central dans le domaine de la sécurité.

Les comités et sous-comités centraux dans le domaine de la sécurité

ISO/TC 8	Navires et technologie maritime	ISO/TC 8/WG 4
ISO/TC 20	Aéronautique et espace	ISO/TC 20/SC 16
ISO/TC 21	Équipement de protection et de lutte contre l'incendie	
ISO/TC 85	Énergie nucléaire, technologies nucléaires, et radioprotection	
ISO/TC 92	Sécurité au feu	
ISO/TC 94	Sécurité individuelle : Vêtements et équipements de protection	
ISO/TC 224	Approvisionnement de l'eau	WG 7 et 11
ISO/TC 262	Risk management	WG 2 à 5
ISO/TC 292	Sécurité et résilience	WG1 à WG6 WG4 fraud protection
ISO/TC 307	Chaîne de blocs et technologies de registre distribué	
ISO/TC 309	Gouvernance des organisations	
ISO/IEC JTC 1	Technologies de l'information	
ISO/IEC JTC 1/SC 17	Cards and personal identification	
ISO/IEC JTC 1/SC 27	Information security, cybersecurity and privacy protection	WG 1 à WG5
ISO/IEC JTC 1/SC 37	Biometrics	
ISO/IEC JTC 1/SC 38	Cloud computing and distributed platform	
ISO/IEC JTC 1/SC 40	IT management services	WG1 à WG4
ISO/IEC JTC 1/SC 41	IOT	

[17] Ibid.

i. L'ISO/IEC JTC1 SC27 IT Security Techniques

Ce comité, conjoint IEC et ISO, est l'un des plus importants en matière de cybersécurité et de protection de l'information. En chiffres, c'est plus de 150 standards publiés à ce jour, 50 pays participants, 20 pays observateurs.

Au niveau interne, il est organisé en cinq groupes spécifiques : ISMS famille 270xx (systèmes de management de la sécurité de l'information), cryptographie, évaluation et certification, applications, protection des données personnelles et biométrie.

Ce groupe gère également les **Critères Communs (ISO/IEC 15408 et 18045)**, en cours de révision, qui constituent une référence mondiale pour l'évaluation de la sécurité des produits informatiques. Les définissent un langage structuré et normalisé permettant d'exprimer, de manière formelle et vérifiable, les exigences de sécurité applicables à une catégorie donnée de produits - par exemple les pare-feu, les cartes à puce, les modules cryptographiques ou les routeurs.

Ce cadre méthodologique repose sur la notion de Profil de Protection (PP), qui décrit les objectifs et les exigences de sécurité d'un type de produit. Une fois évalués et certifiés par un organisme compétent, ces profils deviennent des références normatives sectorielles servant de base à la certification des produits revendiquant une conformité à ces PPs.

À ce jour, il existe plusieurs centaines de Profils de Protection reconnus par les différents schémas nationaux de certification (ANSSI, BSI ou NIST).

Les certifications délivrées selon les Critères Communs peuvent bénéficier d'une reconnaissance mutuelle entre les pays signataires des accords internationaux de reconnaissance (notamment le CCRA - *Common Criteria Recognition Arrangement*), avec toutefois des limitations selon le niveau d'assurance (EAL) visé ou selon que l'évaluation est conduite sous un schéma européen (EUCC) au niveau substantiel ou élevé impliquant une reconnaissance mutuelle entre les 27 états membres.

Finalement, ce groupe effectue aussi un travail important sur la protection des données personnelles. Par exemple, la **norme ISO/IEC 27701** est autoporteuse de la norme ISO/IEC 27001 afin de prendre en compte les exigences du **RGPD (Règlement Général sur la Protection des Données).**

Le point de vue de François Zamora,

Président de la Commission de Normalisation Sécurité de l'Information, Cybersécurité et Protection des données à l'AFNOR

Les normes en cybersécurité, notamment celles issues de l'ISO/IEC JTC1 SC27, jouent un rôle crucial dans la définition de bonnes pratiques et de cadres de référence pour la confiance dans le numérique. Cette confiance s'appuie sur la robustesse, la résilience et leur amélioration continue dans les domaines des infrastructures numériques physiques et logicielles. Cette confiance réside aussi dans la robustesse des usages du numérique face à la désinformation et à la manipulation des intelligences, humaines ou artificielles. Elles favorisent à l'échelle mondiale l'harmonisation des mesures de sécurité et l'amélioration continue de leur mise en œuvre, facilitant la conformité réglementaire selon une approche de gestion des risques. En structurant les processus et en normalisant les contrôles, elles contribuent à renforcer la résilience des organisations face aux cybermenaces. Enfin, leur adoption jusqu'à un niveau stratégique assure la confiance de l'ensemble des parties intéressées, notamment les utilisateurs, des partenaires, et des investisseurs.

ii. ISO TC 292 – Security and Resilience

L'ISO TC 292 « *Security and Resilience* » couvre un champ plus large relatif à la sécurité (infrastructures critiques, sécurité sociétale, gestion de crise, lutte contre la fraude et la contrefaçon, etc.). La France occupe une place importante au sein de ce comité en animant le groupe de travail **WG 6 Protective Security**, dédié principalement aux mesures de lutte contre la malveillance et en siégeant au sein du groupe consultatif de la présidence du comité technique qui contribue à élaborer sa feuille de route stratégique.

iii. Autres structures ISO annexes

Outre les deux comités principaux, plusieurs autres structures de l'ISO participent à la normalisation dans des domaines liés à la sécurité, aux technologies de l'information et à la protection des données. Ainsi, il y a également le SC17 *Cards and personal identification*, le SC37 *Biometrics*, le SC 38 *Cloud Computing and Distributed Platforms*, plus récemment le SC 41 IOT, le SC42 IA (particulièrement important), le SC44 *Privacy for consumers* et le TC 307 blockchain, etc.

b) L'IEC (*International Electrotechnical Commission*) ou CEI (Commission Electrotechnique Internationale)

Conscients dès 1880 de la multiplicité de mesures et des termes qui ralentissent les progrès dans la science électrique, *l'International Electrical Congress* décide de fonder une commission internationale chargée d'établir des mesures pour la classification des appareils et des machines électriques. Fondée en 1906, la CEI (Commission Electrotechnique Internationale) est un organisme international de normalisation qui publie des normes internationales pour toutes les technologies électriques, électroniques et connexes connues sous le nom de « électro technologie » [18].

A l'heure actuelle, la CEI est un comité de normalisation d'ampleur internationale, rassemblant près de 170 pays et environ 30 000 experts. Ces mêmes experts sont choisis par leur comité national (NC) pour partager leur expertise et représenter les exigences nationales au niveau mondial[19].

Les publications de la CEI sont élaborées par plus de 200 comités techniques et sous-comités (TC/SC) et des centaines de groupes de travail, chacun étant responsable d'un domaine technologique spécifique[20]. L'IEC dispose historiquement de deux TC principaux traitant de problèmes de sécurité, mais ce domaine s'étend rapidement avec la généralisation des moyens électroniques (exemple : le TC 79 *Alarm and Electronic Security Systems*, avec la série de normes IEC/EN 60839-11 qui traite de la détection d'intrusion, de la vidéosurveillance et du contrôle d'accès).

[18] IEC, 2026, https://www.iec.ch/understanding-standards.
[19] Ibid.
[20] Ibid.

Les principaux TC de l'IEC dans le domaine de la sécurité

IEC/SC 31J	Classification of hazardous areas and installation requirements		
IEC/TC 57	Power systems management and associated information exchange	IEC 62351 : Data and communication security Development in IEC TC57 WG15 Scope Power Automation and Smart Grids	
IEC/TC 65	Industrial-Process Measurement, Control & Automation	WG10 IEC 62443 : Industrial Automation and Control Systems Security	ISO 62443, ISO 62351
IEC/TC 79	Alarm and electronic security systems		
IEC/TC 89	Fire hazard testing		

c) Union internationale des télécommunications (UIT/ITU)

L'Union internationale des télécommunications est l'agence des Nations unies spécialisée dans les technologies de l'information et de la communication. Créée en 1865 et héritière de l'Union télégraphique internationale, elle est fondée sur le principe de la coopération internationale entre les gouvernements (États membres) et le secteur privé (membres des secteurs, associés et universités), elle regroupe aujourd'hui 194 États membres et 1 000 membres et associés du secteur[21].

L'UIT dispose de plusieurs volets d'actions. Si elle est chargée de la planification des télécommunications au sens large (attributions des fréquences radioélectriques et des orbites de satellites à l'échelle mondiale, compétences dans l'Internet haut débit, navigation maritime et aéronautique, etc.), elle dispose également d'un volet normalisation. Ainsi, elle établit les normes techniques et diffuse les informations nécessaires pour garantir une connexion transparente des réseaux et des technologies[22].

Cette instance de normalisation a également des groupes chargés de la sécurité : l'ITU-T SG17 et le 3GPP SA3.

[21] ITU, https://www.itu.int/en/about/Pages/default.aspx#/fr.
[22] Ibid.

Les principaux TC de l'ITU dans le domaine de la sécurité

ITU-T-SG2	Operational aspects.	
ITU-T-SG13	Future networks, with focus on IMT-2020, cloud computing and trusted network infrastructures	
ITU-T-SG15	Transport, Access and Home	
ITU-T-SG17	Security	
ITU-T-SG20	Internet of things (IoT) and smart cities and communities (SC&C)	

2. Les comités de normalisation européens

Le point de vue d'Alban Feraud,

IN Groupe

Au cours des dernières années, la Commission Européenne a mis l'accent sur la règlementation du numérique au travers de nombreuses initiatives législatives majeures (NIS2, CRA, AI Act, DORA, eIDAS, DSA, DMA, digital omnibus...). Ces textes visent à assurer l'accès à tous au numérique, la transparence du numérique vis-à-vis des citoyens, la protection des droits et libertés publiques dans le monde numérique, et un haut niveau de confiance, de cybersécurité ou de résilience du numérique dans l'espace Européen, ce qui par nature nécessite une harmonisation technique de sorte à assurer une mise en application uniforme. Afin d'atteindre cette harmonisation pan-Européenne, des standards techniques précis, clairs et à l'état de l'art sont nécessaires.

Ainsi, derrière chacune de ces initiatives se cachent des travaux de standardisation intenses et approfondis réunissant de très nombreux experts. A ce jour, les experts européens en normalisation du numérique sont largement accaparés par ces travaux car ces derniers sont non seulement importants mais aussi concomitants. Dans un contexte où l'Europe semble ouvrir les yeux sur son absence d'autonomie technologique dans le domaine numérique, il est crucial

que ces standards techniques autorisent cette autonomie technologique. Cela nécessite entre autres qu'ils soient indépendants de technologies ou de standards non européens ou non issus des organisations de standardisation internationales (ISO, IEC, ITU), mais aussi qu'ils soient élaborés par des structures réellement Européennes (entreprises et organisations) de sorte à refléter les intérêts de Etats membres.

Le cadre législatif européen : un rôle structurant pour la normalisation

La législation européenne (réglementations et directives) fait office tant de moteur que de cadre pour orienter les travaux de normalisation. La normalisation devient alors un outil pour se conformer à la législation européenne : les normes servent de support technique pour démontrer la conformité. On peut dire qu'elles traduisent et opérationnalisent les exigences des textes législatifs comme eIDAS, NIS, RGPD, ou CSA qui ont alors un impact direct sur les normes élaborées.

Via la directive NIS 2, le CEN, le CENELEC et l'ETSI développent des normes sur la gestion des risques, la notification des incidents, la résilience des infrastructures.

Autre exemple, le Cyber Security Act (CSA) redessine et réorganise la gouvernance pour la cybersécurité mais aussi la normalisation. Il impose des acteurs clés :

- ENISA, l'agence européenne pour la cybersécurité, joue un rôle central dans la certification.
- ECCG (European Cybersecurity Certification Group) regroupe les autorités nationales de cybersécurité, assure la coordination des schémas de certification.
- SCCG (Stakeholder Cybersecurity Certification Group) représente les parties prenantes (industrie, société civile, recherche).
- DG CONNECT (Commission européenne) dispose d'une forte influence dans la stratégie et le pilotage.

L'Europe reconnait trois ESO (*European Standardisation Organisation*) en charge de la normalisation, à savoir le CEN (Comité Européen de Normalisation), le CENELEC (Comité Européen de Normalisation Électrotechnique), et l'ETSI (*European Telecommunications Standards Institute*).

a) CEN et CENELEC

Le **CEN (Comité Européen de Normalisation**) et le **CENELEC (Comité Européen de Normalisation Électrotechnique)** travaillent à l'élaboration et à la définition de normes européennes larges pour répondre aux besoins identifiés et à soutenir la mise en œuvre de la législation européenne.

Les travaux de normalisation peuvent être demandés par mandat de la Commission européenne ou de l'Association Européenne de Libre Echange - AELE (ce qui représente environ 30% des cas) ou par les membres eux-mêmes (soit les organismes nationaux de normalisation). Enfin, ils peuvent parfois se faire à la demande d'autres parties prenantes (notamment les associations professionnelles, ONG, etc.)[23].

Le système d'élaboration des normes est **décentralisé** (au travers d'un large éventail d'acteurs) et repose sur un processus **collaboratif** ce qui garantit que les normes soient consensuelles et représentent les intérêts de toutes les parties [24]. Les membres constitués des **organismes nationaux de normalisation (NSB)**[25] pour le CEN, et des **comité nationaux (NC)** pour le CENELEC permettent à chaque pays de l'UE et de l'AELE de participer. Ces organismes gèrent les groupes techniques qui élaborent les normes et le centre de gestion CEN-CENELEC à Bruxelles gèrent et coordonnent ce système.

Un large éventail de parties prenantes participe aux activités de normalisation (industriels, pouvoirs publics, associations professionnelles, syndicats, établissements d'enseignement, organismes de recherche, etc.).

Les différents groupes du CEN-CENELEC dans le domaine de la sécurité

CEN/CLC/ETSI/SF-SSCC	CEN-CENELEC-ETSI Sector Forum on Smart and Sustainable Cities and Communities	Regulation (EU) 2016/679 of the European Parliament and the Council on the protection of natural people with regards to the processing of data and on the free movement of such data (pdf format)
CEN/CLC/TC 4	Services for fire safety and security systems	

[23] Site du cenelec. https://www.cencenelec.eu/european-standardization/european-standards/..
[24] Ibid.
[25] Ces organismes nationaux de normalisation sont au nombre de 43 et sont tous issus de 34 pays européens (États membres de l'UE, et autres du marché unique européen).

CEN/CLC/JTC 13	Cybersecurity and data protection	WG1 chair advisory WG2 ISMS WG3 evaluation certification WG4 disbanded/clos WG5 privacy WG6 Product security WG8 RED WG9 CRA (Vulnerability handling) WG10 cryptography
CEN/CLC/JTC21	IA	WG5 Security
CEN/CLC/JTC24	Digital Product passport	
CEN/CLC/JTC25	Data, data spaces and Edge	
CEN/TC 70	Manual means of fire fighting equipment	
CEN/TC 72	Fire detection and fire alarm systems	20 WG
CEN/TC 79	Respiratory protective devices	
CEN/TC 85	Eye protective equipment	
CEN/TC 158	Head protection	
CEN/TC 159	Hearing protectors	
CEN/TC 160	Protection against falls from height including working belts	
CEN/TC 161	Foot and leg protectors	
CEN/TC 162	Protective clothing including hand and arm protection and lifejackets	
CEN/TC 164	Water supply	11 WG
CEN/TC 224	Personal identification and related personal devices with secure element, systems, operations and privacy in a multi sectorial environment	
CEN/TC 212	Pyrotechnic articles	
CEN/TC 239	Rescue systems	
CEN/TC 278	Intelligent transport systems	15 WG WG5: Traffic control
CEN/TC 325	Crime prevention through building, facility and area design	
CEN/TC 391	Social and citizen security	
CEN/TC 419	Forensic science services	
Cenelec/BTTF 133-1	Sound systems for emergency purposes which are not part of fire detection and alarm systems	
Cenelec/BTTF 69-3	Road traffic signal systems	
Cenelec/SR 103	Transmitting equipment for radiocommunication	
Cenelec/TC 205	Home and Building Electronic Systems (HBES)	
Cenelec/TC 79	Alarm systems	10 WG

b) ETSI

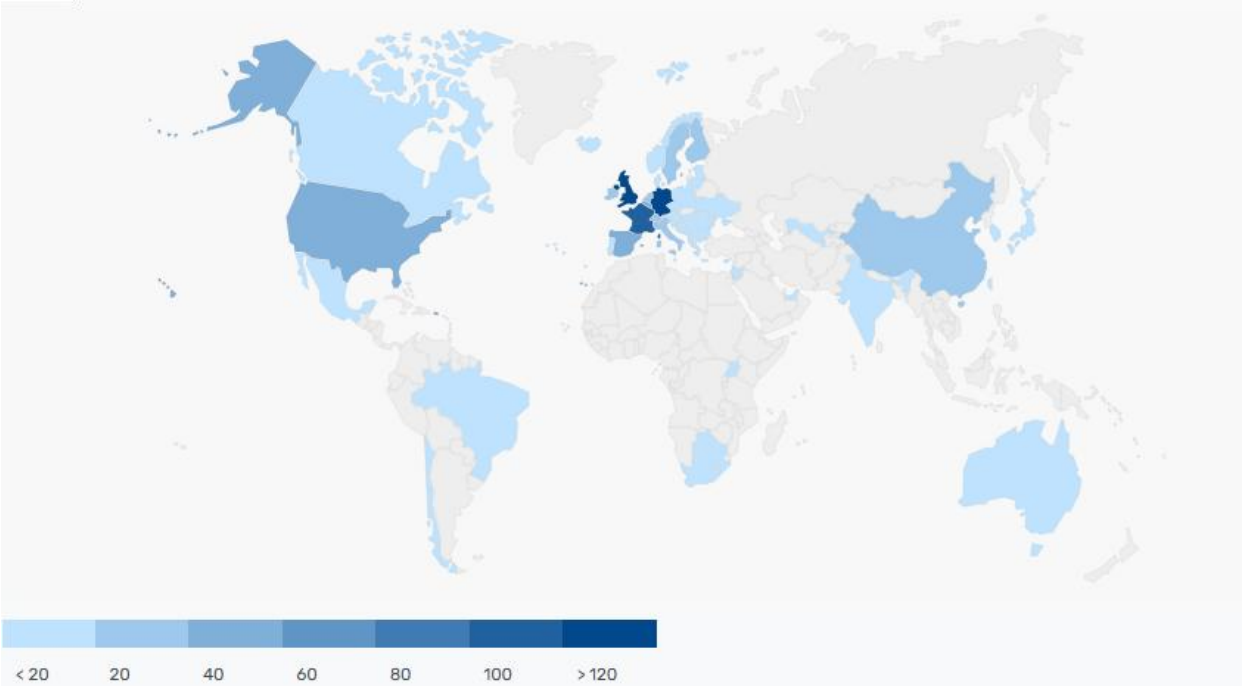

Figure 2 : Les membres ETSI à travers le monde (Source : ETSI, 2026).

Fondée en 1988, ETSI (*European Telecommunications Standards Institute*) a pour objectif l'élaboration de normes applicables à l'échelle mondiale relatives aux Technologies de l'Information et de la Communication (TIC) et plus particulièrement aux réseaux et services de télécommunications, de radiodiffusion et d'autres communications électroniques. Essentiellement pilotée par les industriels membres de l'ETSI, elle est en majorité financée par ses membres, puis par l'UE. Bien qu'elle soit un organisme fondé pour répondre aux besoins européens, ETSI a dépassé son cadre régional et regroupe aujourd'hui plus de 900 organisations originaires de plus de 60 pays et de cinq continents[26].

Contrairement au fonctionnement stato-centré du CEN/CENELEC, les TC ETSI sont pilotés par les membres essentiellement industriels. Mais la gouvernance a été revue récemment pour renforcer la position des Etats. Parmi les *Technical Comittee* (TC), le TC *Cybersecurity* de l'ETSI traite les sujets suivants : *post*

[26] ETSI, https://www.etsi.org/about.

quantum computing, *security assurance by default*, *cybersecurity consumer IOT*, *structured information sharing*, *CIS controls*, etc.

Les principaux TC de l'ETSI

ETSI TC Cyber	Cybersecurity	WG EUSR, WG QSC	Quantum safe cryptography
ETSI TC ESI	Electronic signature		eIDAS, E Wallet
ETSI TC LI	Lawful interception		
ETSI TC TCCE	Tetra	WG6 security	

3. Les acteurs nationaux de la normalisation

Plusieurs acteurs à l'échelle nationale agissent sur le territoire français en matière de normalisation.

a) AFNOR

L'AFNOR (Association Française de Normalisation) est l'organisme national de normalisation (National Body - NB) pour la France. Avec environ 2 000 normes homologuées par an, elle est en charge de la coordination et de l'animation du système français de normalisation, tient à jour le catalogue des normes françaises homologuées et organise des consultations publiques sur chaque projet de norme.

Elle porte les positions françaises au niveau européen (CEN CENELEC) et international (ISO, IEC) [27]. L'AFNOR est membre du CEN et de l'ISO. Le Comité Électrotechnique Français (AFNOR-CEF) représente la France au sein du CENELEC et de l'IEC (*International Electrotechnical Commission*).

b) ANSSI

L'Agence nationale de la Sécurité des Systèmes d'Information (ANSSI), sous l'autorité du Secrétariat Général à la Défense et à la Sécurité Nationale (SGDSN) est l'autorité nationale en matière de cybersécurité. À travers ses différents

[27] Ministère de l'économique de l'industrie et du numérique, 2016, https://www.entreprises.gouv.fr/files/files/Publications/2016/guides/2016-guide-pratique-du-bon-usage-de-la-normalisation-dans-la-reglementation.pdf.

schémas de qualification (PASSI, PDIS, PACS, PAMS, etc.) et de certification des solutions de cybersécurité, elle contribue au développement et à la reconnaissance de standards français, européens et internationaux.

c) CSF et commission NORSEC

Le Comité Stratégique de Filière (CSF) industries de sécurité anime un groupe de travail dédié à la normalisation NORSEC (normalisation en matière de sécurité). Le comité informel NORSEC a été créé pour répondre à un enjeu de souveraineté nationale ; cela offre la possibilité aux experts français présents dans les différentes instances de normalisation de se coordonner pour définir une position stratégique commune. NORSEC regroupe des acteurs étatiques (SGSN, ANSSI, MI, DGE), et privés, notamment industriels (grands groupes, ETI et PME), ainsi que leurs organisations professionnelles (ACN, GICAT, ...). Son secrétariat est actuellement assuré par l'ACN.

d) Bureaux de Normalisation Sectoriels (BNS)

Les Bureaux de Normalisation Sectoriels sont des organismes spécialisés qui agissent par délégation de l'AFNOR. Ils coordonnent et animent des travaux de normalisation dans leurs domaines respectifs en réunissant les acteurs publics et privés concernés. Leurs commissions de normalisation contribuent à l'élaboration du cadre normatif national mais aussi européen et international.

4. Les autres comités de normalisation

En plus de ces comités précédemment listés, qui fonctionnent à des échelles précises, il existe un grand nombre de forums industriels thématiques. Ces comités développent des standards « de facto » qui sont des accords entre industriels et qui dans certains cas sont ensuite repris par un comité de standardisation officiels. On peut citer en particulier TCG, OASIS, etc.

Les forums industriels informels de normalisation

OASIS	Organization for the Advancement of Structured Information Standards	
OACI		NTWG
IEEE		Industry Connections Security Group (ICSG)
TCG	Trusted Computing Group	12 WG
Open group		
Global Platform		
W3C	World Wide Web Consortium	
FIDO Alliance	Open, interoperable standards for secure, passwordless authentication using strong cryptographic credentials	
Open Forum	Open source	
SPAC Alliance	Smart Physical Access Control Alliance	SSCP (Smart & Secure Communication Protocol) – Industrial Standard

5. Coopération entre SDO (*Standard Development Organization*)

Mais les limites et frontières entre les SDO ne sont pas si fixes. Outre les membres du CEN et/ou du CENELEC, les comités techniques de ces deux organisations européennes intègrent aussi des observateurs parfois issus de l'ISO et de la CEI. En parallèle, tous les membres nationaux du CEN et du CENELEC sont également membres de l'ISO ou de la CEI. Cette double présence permet que les intérêts des acteurs européens soient pris en compte à l'échelle internationale et vice-versa[28].

De plus, il existe différents modes de coopération entre SDO. Au niveau européen, la coopération est coordonnée par le groupe conjoint des présidents (JPG). Comme son nom l'indique, la JPG comprend les présidents et vice-présidents du CEN et du CENELEC et leurs équivalents ETSI (Présidents de l'Assemblée générale et Vice-Présidents, et Président du Conseil d'administration de l'ETSI), ainsi que le Directeur général du CEN et du CENELEC et le Directeur général de l'ETSI[29].

[28] Site du CENELEC, https://www.cencenelec.eu/european-standardization/european-standards/.
[29] Ibid.

Plus globalement, on constate différentes dynamiques. La tendance est de regrouper des travaux communs sous la forme de JTC (*Joint Technical Committee*) entre SDO pour faciliter la coopération et éviter les duplications d'efforts. D'autre part, il existe des accords de reconnaissance entre SDO (*Francfort, Vienna et Dresden agreement*). Le CEN collabore avec l'ISO conformément aux dispositions de l'Accord de Vienne, tandis que le CENELEC travaille en étroite collaboration avec la Commission Electrotechnique Internationale (CEI) par l'intermédiaire de l'Accord de Francfort. Ces accords de reconnaissance permettent de reprendre tel quels des standards développés dans un autre comité comme ce que fait le JTC13[30].

a) JTC 21 (Intelligence artificielle)

Le JTC21 a été créé en 2021 par le CEN et CENELEC. Avec une approche inclusive et fondée sur le consensus, les normes sont élaborées sous mandat de la Commission européenne. Cette création émane du besoin d'élaborer des normes européennes harmonisées, en lien avec le règlement européen *IA act*. Les entreprises qui respectent ces normes harmonisées bénéficieront d'une présomption légale de conformité avec les exigences de la loi sur l'IA[31].

Avec 300 experts provenant de plus de 20 pays, répartis dans cinq groupes de travail, le JTC21 couvre une pluralité de domaines : aspects stratégiques, opérationnels, sociétaux, ingénierie, cybersécurité des systèmes IA.

Il faut noter que les risques de conflit avec le JTC13 sur les aspects cybersécurité sont possibles. Toutefois, une collaboration institutionnalisée s'est mise en place, le JTC 21 prévoit une coopération avec JTC 13, ainsi que l'ETSI et l'ENISA pour aligner les travaux en matière de cybersécurité des IA[32].

[30] Le JTC 13 CEN CENELEC cybersécurité et data protection assure une coordination des travaux au sein du CEN CENELEC et assure en particulier la transposition des standards SC27, 6 WG.
[31] CENELEC, 2024,https://jtc21.eu/about/.
[32]Portail qualité LU, La normalisation européenne en matière d'intelligence artificielle : un support pour le cadre législatif, 2023, https://portail-qualite.public.lu/fr/actualites/normes-normalisation/2023/normalisation-europeenne-matiere-intelligence-artificielle-support-cadre-legislatif.html.

Le point de vue de Nicolas Scuto,

Ministère de l'Intérieur

Le rôle du ministère de l'Intérieur dans les normes de sécurité et résilience

Dans le contexte d'instabilité politique internationale et d'hypercompétition économique (concentration, rachat, ingérence privée et gouvernementale, etc.), de judiciarisation des affaires (corruption, embargo, fraude fiscale, blanchiment, etc.), les acteurs socio-économiques, et les entreprises en premier lieu, sont vulnérables. Or, d'une part, l'état de l'art de la sûreté, au sens de la lutte contre les actions malveillantes, est encore en développement ; d'autre part, la sûreté en entreprise est considérée comme une activité improductive.

En matière de politique publique, la sécurité sociétale reste l'objectif prioritaire pour l'état. On note toutefois une évolution du corpus législatif en matière de politique de prévention notamment dans le domaine de la protection du secret de la défense nationale, de sécurité des activités d'importance vitale et de protection des entités critiques contre les ingérences étrangères. Ce corpus est complété par la jurisprudence qui fait état par exemple d'une obligation de moyens de sécurité renforcée[33] pour les collaborateurs en déplacement à l'étranger.

La commission de normalisation Afnor CN Sécurité et Résilience, présidée par le ministère de l'intérieur, est mise à contribution pour compléter cette réponse règlementaire d'un corpus de bonnes pratiques. Elle est la structure miroir des instances CEN/TC 391 Societal and Citizen Security et surtout de l'ISO/TC 292 Security and resilience. Celles-ci ont pris une pleine part dans l'élaboration d'un corpus de normes visant à définir et mettre en œuvre une politique de sûreté préventive en insistant sur les liens avec la continuité d'activité, la gestion de crise, la résilience des communautés et la cybersécurité.

[33] Arrêt Air France, 2015, https://www.legifrance.gouv.fr/juri/id/JURITEXT000033154104/.

Figure 3 : Périmètre du management de la sureté (draft NF ISO 22340 Architecture de la sûreté - source : ministère de l'intérieur)

La figure ci-après illustre les liens organisationnels et managériaux à considérer du point de vue du management de la sûreté. La flèche rouge matérialise l'activité d'entrée du management de la sûreté, à savoir le processus d'évaluation du risque de sûreté. Puis une contribution à la continuité d'activité (protection des actifs stratégiques), à la gestion de crise (protection de la cellule de crise, personnes, infrastructures et logistique). Enfin, une contribution à la résilience des populations en cas d'incident grave (exemple : terrorisme, accident industriel, catastrophe naturelle). Le schéma ci-dessous a initié l'élaboration de la norme NF ISO 22342 - Sécurité et résilience – lignes directrices pour la sûreté des sites, dont l'élaboration à l'ISO/TC 292 a été pilotée par un expert de la DEPSA, au sein du groupe de travail 6, animé par la France.

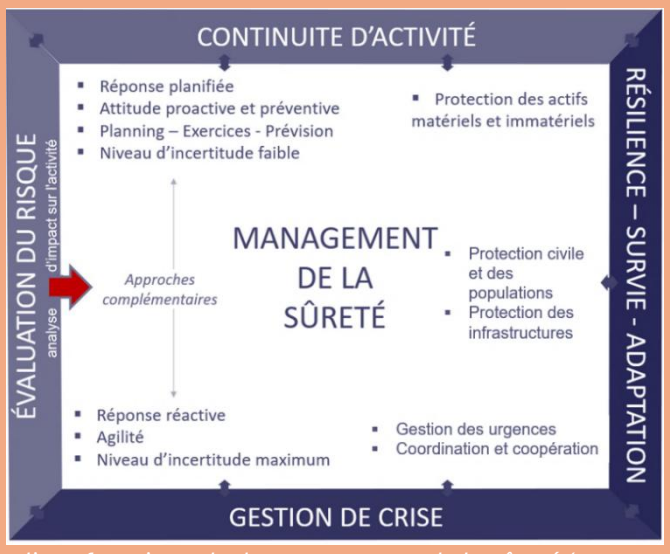

Figure 4 : illustration des liens fonctionnels du management de la sûreté (source : Jean-Marc Picard, UTC - 2020).

i. Principales normes en sûreté et continuité d'activité

Les normes suivantes sont soutenues activement par le ministère de l'intérieur, soit pour leur caractère fondamental (norme de vocabulaire et de concepts), soit organisationnel (normes de management).

Vocabulaire de la sûreté :

***L'ISO 22300 - Sécurité et résilience - Vocabulaire** définit des termes et concepts relatifs aux thèmes de la sécurité et de la résilience. Elle est consultable gratuitement.*

Architecture et plan de sûreté :

***L'ISO 22340 - Sécurité et résilience - Architecture de la sûreté** et **l'ISO 22342 - Sécurité et résilience – lignes directrices pour la sûreté des sites** donnent un cadre pour organiser et élaborer les activités de sûreté. Ces normes auxquels ont contribué activement les experts français, dont ceux du ministère de l'intérieur, insiste particulièrement sur la définition d'un processus de gouvernance de la sûreté et de gestion des risques de sûreté.*

Afnor Spec 2404 - Plan de sûreté - Exigences opérationnelles :

En 2025, le ministère de l'intérieur a piloté un groupe d'experts publics et privés qui a élaboré les exigences fondamentales pour élaborer un premier plan de sûreté. Ce document destiné notamment aux TPE, PME et ETI est le référentiel de base dans le dispositif Pacte sûreté du ministère de l'intérieur en cours d'élaboration. Ce référentiel est gratuit au téléchargement et à l'usage.

Continuité d'activité et résilience organisationnelle :

***L'ISO 22301 systèmes de management de la continuité d'activité** cadre l'analyse d'impact, les plans de continuité et la reprise des activités essentielles dont les services de sûreté publique et est certifiante.*

***L'ISO 22313 - Lignes directrices pour ISO 22301** et suivantes renforcent la préparation, la gestion de crise et le retour à une situation nominale.*

Gestion de crise :

***L'ISO 22361 Crisis management - Guidelines** recommande une stratégie capacitaire qui consiste à préparer les processus qui seront utiles durant une crise (ex. : prise de décision, formation, communication, retour d'expérience).*

***L'Afnor spec X52-315_2020 - Préconisations pour la conception et le maintien en condition opérationnelle des centres de crise** recommande une démarche de conception et d'exploitation d'un centre de crise. Elle préconise également de missionner un régisseur chargé de garantir un centre opérationnel en 24/7.*

ii. Focus sur la résilience des entités critiques en lien avec la directive REC de l'Union Européenne

La directive REC (UE) 2022/255734 sur la résilience des entités critiques, en tant que fournisseurs de services essentiels, impose trois principales obligations aux États membres :

- *Développer une stratégie nationale,*
- *Évaluer les risques auxquels les entités critiques sont exposées, et*
- *Identifier ces entités.*

En juin 2025, un ensemble de normes volontaires a été identifié par les membres de la commission de normalisation Afnor CN Sécurité et Résilience présidée par la DEPSA. Ces référentiels ISO constitueraient un portfolio de base pour une première réponse organisationnelle et managériale aux exigences de résilience de la directive REC. La cartographie élaborée présentée ci-après agence ces normes au gré de leur utilité, globale ou par secteur critique ; elle mentionne également les référentiels français élaborés par le secrétariat général de la défense et de la sécurité nationale (SGDSN) en matière de sécurité des activités d'importance vitale (SAIV).

Figure 5 : Principales normes de management ISO pour mettre en œuvre la directive REC (UE) 2022/2557 (source : Afnor et ministère de l'intérieur - juin 2025).

[34] Union européenne, EUR-Lex, 2022,https://eur-lex.europa.eu/eli/dir/2022/2557/oj?locale=fr.

iii. ETSI : normalisation européenne en sécurité et résilience des réseaux et services

L'ETSI produit des normes et spécifications pour la sécurité des réseaux et services de communications électroniques (ex. : télécoms, 5G, IoT, services numériques), qui conditionnent la disponibilité et l'intégrité des communications de sécurité civile et des services aux citoyens. Le ministère de l'intérieur contribue activement à l'élaboration de certaines normes pour les propres besoins de ses forces de sécurité intérieure.

iv. Besoins et perspectives au niveau français

Evaluation de la conformité en sûreté :

Ce processus est fondamental pour toute entité qui souhaite démontrer que sa gestion de la sûreté est structurée et alignée avec la stratégie de l'entreprise. Il s'agit aussi d'un enjeu d'opposabilité juridique. L'Afnor spec 2404, avec ses exigences, apporte une première contribution à ce processus.

Projet sur les critères de performance de la sûreté :

Pour aider les responsables de la sûreté des entreprises, le ministère de l'intérieur a initié une réflexion à l'ISO/TC 292 et à la CN Sécurité et Résilience Afnor visant à élaborer les critères et leurs caractéristiques d'indicateurs du management de la sûreté.

v. Articulation globale sûreté physique – cyber – continuité

Les normes de management (ISO 27001, ISO 22301, ISO 22342 et guides AFNOR associés) fournissent un socle commun de gouvernance des risques, qui relie directement sûreté des sites, cybersécurité des systèmes et continuité des services aux citoyens.

Les normalisations européennes (CEN-CENELEC) et télécoms (ETSI) complètent cet ensemble en cadrant la sécurité des infrastructures et des services numériques, ce qui renforce la capacité à gérer les crises hybrides (physiques et cyber) et à assurer une résilience globale au bénéfice de la sécurité du citoyen. Cette coordination est l'expression de la demande de structuration cohérente de la commission européenne en matière d'outils de protection des actifs dans l'espace Schengen : elle est prise en compte par la DEPSA dans ses activités normatives et opérationnelles, au sein du ministère de l'intérieur et au niveau interministériel au sein du groupe interministériel aux normes (GIN), dirigée par la sous-direction de la normalisation, de la règlementation des produits et de la métrologie (SQUALPI), structure de la direction générale des entreprises (DGE).

vi. Perspectives

Dans le contexte socio-économique et géopolitique actuel marqué par une forte instabilité due aux menaces (de guerre) hybrides, plusieurs pistes de réflexion sont engagées en normalisation de la sécurité et résilience en 2026.

La première consiste à prendre en compte les ***ressources capacitaires*** *dans l'élaboration d'un plan de sûreté et de continuité d'activité, idéalement au niveau européen, dans le contexte de la mise en œuvre normative de la directive REC.*

La deuxième est la conséquence de la première, à savoir évaluer la pertinence de faire évoluer le modèle de gouvernance en matière de protection de l'entreprise vers une ***direction de la résilience*** *qui engloberait la gestion de la sûreté, des risques, de la continuité d'activité et de la crise (cf. Figure 2).*

La troisième vise à renforcer la protection juridique des entreprises par l'évaluation de la conformité aux normes volontaires idoines.

Le ministère de l'intérieur est partie prenante de la normalisation des activités de sûreté non seulement pour ses besoins internes mais également pour contribuer à la protection des intérêts économiques de la nation. Son engagement depuis plus de 20 ans dans les instances de normalisation françaises, européennes et internationales témoignent de sa motivation à soutenir un écosystème malheureusement encore trop peu présent pour influencer les normes volontaires qui pourtant les concernent. La demande de normalisation issue de la directive REC et les pistes de réflexion exposées pourraient constituer des leviers pour stimuler l'implication de nouvelles parties prenantes.

III. Les normes de sécurité de l'information

1. Les normes internationales

a) Les normes ISO

La norme ISO définit la gestion, les services, la fourniture de matériel ou l'élaboration d'un produit.

L'ISO élabore des normes à travers un processus consensuel impliquant des comités techniques. Ces comités techniques sont composés d'experts indépendants, de différents pays et secteurs et de divers membres.

L'élaboration d'une norme ISO débute par la création d'un projet qui répond à une demande spécifique du marché. Le processus de vote est essentiel pour atteindre un consensus sur un projet de norme ISO. Le processus d'élaboration d'une norme ISO s'étend généralement sur une période de trois ans, de la proposition initiale à sa publication.

Depuis sa création, on compte 24 500 normes internationales ISO publiées qui couvrent un large éventail de domaines[35]. Ces normes sont souvent harmonisées avec IEC, car beaucoup sont copubliées. Voici plusieurs des groupes thématiques sous lesquels sont catégorisées ces normes.

Système de management de la sécurité de l'information (SMSI)

La famille 270xx représente l'essentiel de cette catégorie :

- ISO/IEC 27000:2014 « Systèmes de management de la sécurité de l'information – Vue d'ensemble et vocabulaire »
- ISO/IEC 27001:2013 « Systèmes de management de la sécurité de l'information – Exigences »
- ISO/IEC 27002:2013 « Code de bonnes pratiques pour le management de la sécurité de l'information »
- ISO/IEC 27003:2010 « Guidance »
- ISO/IEC 27004:2009 « Monitoring, measurement, analysis and evaluation »
- ISO/IEC 27005:2011 « Gestion des risques en sécurité de l'information »

À savoir : Il existe aussi des normes spécifiques par secteur (énergie, finances, cloud…)

[35] ELI, https://www.eliapp.io/blog/iso-normes-incontournables-pour-la-qualite-et-la-securite.

Zoom : ISO/IEC 27001

Norme appliquée internationalement, elle définit les exigences auxquelles un système de management de la sécurité de l'information (SMSI) doit se conformer. La norme ISO/IEC 27001 fournit aux entreprises de toutes tailles, quel que soit leur secteur d'activité, un cadre normatif pour l'établissement, la mise en œuvre, la tenue à jour et l'amélioration continue d'un SMSI. Face à l'essor de la cybercriminalité et à l'émergence constante de nouvelles menaces, une approche holistique de la sécurité de l'information est nécessaire, comme le fait ISO/IEC 27001. Cette approche est fondée sur des procédures de contrôle dans le but d'anticiper, gérer et réduire les risques liés à la sécurité des données[36].

Cryptographie et mécanismes de sécurité

Ces normes définissent les mécanismes de protection technique comme le chiffrement, la signature ou la génération aléatoire. Elles sont essentielles pour garantir la confidentialité, l'intégrité et l'authentification des données.

Il s'agit-là des mécanismes cryptographiques suivants :

- ISO/IEC 18033 : « Algorithmes de chiffrement – Partie 1 à 5 ».
- ISO/IEC 9798-2 : 2008 « Authentification d'entité – Partie 1 à 6 ».
- ISO/IEC 14888-1 : 2008 « Signatures numériques avec appendice – Partie 1 à 3 ».
- ISO/IEC 18031 : 2011 « Génération de bits aléatoires ».

Méthodes d'évaluation de la sécurité

Les normes ISO relatives aux méthodes d'évaluation de la sécurité définissent un cadre méthodologique (niveaux de sécurité, gestion des risques, validation) applicables selon le secteur concerné (automobile, numérique, etc.). Elles recommandent des méthodes d'évaluation de la sécurité allant des analyses qualitatives aux approches quantitatives.

Ce sont par exemple les critères communs :

- ISO/IEC 15408 : 2009 « Critères d'évaluation pour la sécurité TI – Partie 1 à 3 »
- ISO/IEC 18045 : 2008 « Méthodologie pour l'évaluation de la sécurité des TI »

[36]ISO,https://www.iso.org/fr/home.html#:~:text=ISO%20%3A%20Des%20normes%20mondiales%20pour,aux%20entreprises%20et%20aux%20consommateurs.

Et les normes spécifiques :

- ISO/IEC 19790 : 2012 « Exigences de sécurité pour les modules cryptographiques ».
- ISO/IEC 24759 : 2013 « Spécifications de tests pour les modules cryptographiques ».
- ISO/IEC 17825 : « Définition des métriques de tests pour les attaques non invasives ».
- ISO/IEC 18367 : « *Cryptographic algorithms and security mechanisms conformance testing* ».

Zoom : ISO/IEC 15408 (Common Criteria)

Cette norme élabore des critères communs qui doivent assurer la sécurité des technologies de l'information. Ainsi, elle fournit une méthodologie structurée pour définir, évaluer et certifier la sécurité des produits IT. Elle est notamment utilisée pour les certifications EAL (*Evaluation Assurance Level*).

Contrôles et services de sécurité

Ces normes touchent essentiellement aux domaines des applications et des services et incluent :

- ISO/IEC 27033 : « Network security – Part 1 à 6 ».
- ISO/IEC 27034 : « Application security – Part 1 à 7 ».

Gestion d'identités et technologies de domaine privé dont la biométrie et la privacy

Il existe aussi plusieurs normes chargées de définir les cadres et critères visant à encadrer les domaines suivants : la gestion d'identité, la biométrie, la protection des données personnelles et les technologies de domaine privé.

- ISO/IEC 29100 : 2011 « *A privacy framework* ».
- ISO/IEC 29134 : « *Privacy Impact Assessment Methodology* ».
- ISO/IEC 29151 : « *Code of Practice for PII protection* ».
- ISO/IEC 29190 : « *Privacy capability assessment model* ».
- ISO/IEC 29191 : « *Requirements for partially anonymous, partially unlinkable authentication* ».
- ISO/IEC 24760 : « *A framework for identity management* ».
- ISO/IEC 24745 : « *Biometric template protection* ».

b) Les normes IEC

Le point de vue de Jean-François Sulzer,

Représentant Thales au début des travaux, puis consultant indépendant

Les attaques terroristes qu'a malheureusement connues la France au cours des 25 dernières années, alors que les caméras de vidéosurveillance ne cessaient de se multiplier, ont mis en évidence le besoin pour les forces de sécurité de pouvoir exploiter en temps réel, comme en différé, toutes ces images, alors que dans un même lieu, comme une gare, elles peuvent provenir de systèmes différents, fixes et mobiles (comme à bord de bus, métros ou trains). Pour qu'une même scène puisse être suivie par plusieurs de ces caméras, il faut, au-delà de savoir lire les données, être capable d'en géolocaliser la source avec précision en 3D, d'en dater de façon absolue l'instant de capture, d'en vérifier l'authenticité, etc. Ce besoin (en fait mondial) d'interopérabilité fine, en des lieux et instants imprévisibles, portant sur des produits et solutions fabriquées dans le monde entier, ne pouvait trouver de réponse que dans une norme internationale. Nous nous sommes donc retrouvés (ministère de l'Intérieur, RATP, SNCF et les acteurs de la filière) d'abord à l'AFNOR pour formaliser la demande de norme, puis à l'IEC où nous avons été rejoints par différents acteurs mondiaux pour démarrer le développement de la norme IEC 62676 - 2 - 11, dont j'ai été le chef de projet jusqu'à sa promulgation en mai 2024.

Les normes IEC élaborent un cadre garantissant la sécurité, l'interopérabilité et la fiabilité des processus faisant appel aux technologies électriques, et électroniques[37].

Bien que l'adoption des normes IEC soit volontaire, elles sont souvent adoptées par les pays ou les régions pour devenir des normes nationales ou régionales si bien que 80 % des normes européennes en matière d'électricité et d'électronique sont conformes aux normes internationales CEI[38].

[37] Magnectic Innovations, https://www.magneticinnovations.com/fr/faq-3/que-sont-normes-iec/.

[38] IEC,https://iec.ch/understanding-standards.

Le nombre de normes publiées depuis la création de l'IEC jusqu'en 2024 s'élève à 7617 avec 522 spécifications techniques et 738 rapports techniques.

Chaque norme IEC est publiée sous forme suivante : IEC XXXX (par ex. IEC 62443), ou parfois sous cette forme : IEC/ISO XXXX, si c'est une norme conjointe avec l'ISO.

Alarmes et sécurité

En miroir de l'IEC TC79 (et du CENELEC TC 79), la structure UF 79 de l'AFNOR est chargée de la normalisation des systèmes d'alarme (détection, alarmes incendie, vidéo-surveillance, alarmes anti-hold-up) qui font appel aux électro-technologies.

Electrotechnique et sécurité électrique

- IEC 60364 : installations électriques basse tension.
- IEC 60950 (remplacée par IEC 62368-1) : sécurité des équipements IT.
- IEC 60204 : sécurité des machines (équipements électriques).
- IEC 62368-1 : sécurité équipements IT/AV.
- IEC 60364 : installations basse tension.

Electrotechnique et compatibilité électromagnétique (CEM)

- IEC 61000 : normes de compatibilité électromagnétique (immunité, émissions).
- IEC 60050 : vocabulaire électrotechnique international.

Energie et environnement

- IEC 61850 : communication dans les réseaux électriques intelligents (*smart grids*).
- IEC 61400 : normes pour les éoliennes.
- IEC 62619 : sécurité des batteries lithium pour applications industrielles.

Technologies numériques et cybersécurité

- IEC 62443 : sécurité des systèmes d'automatisation et de contrôle industriels (cybersécurité OT).
- IEC 62351 : sécurité pour les réseaux électriques (*smart grid*).

Electromobilité et transport

- IEC 61851 : systèmes de recharge des véhicules électriques.
- IEC 62196 : connecteurs de recharge.
- IEC 62960 : fiabilité.

c) Les normes IUT

Les normes internationales produites par l'ITU-T, appelées « recommandations » existent au nombre de 4 000.

Ces recommandations s'adressent au domaine des télécommunications, et plus précisément l'architecture et la sécurité des réseaux, les lignes d'abonné numérique large bande, les systèmes de transmission optique (Gbit/s), les réseaux de prochaine génération (NGN) et les questions relatives au protocole IP[39].

2. Les normes européennes

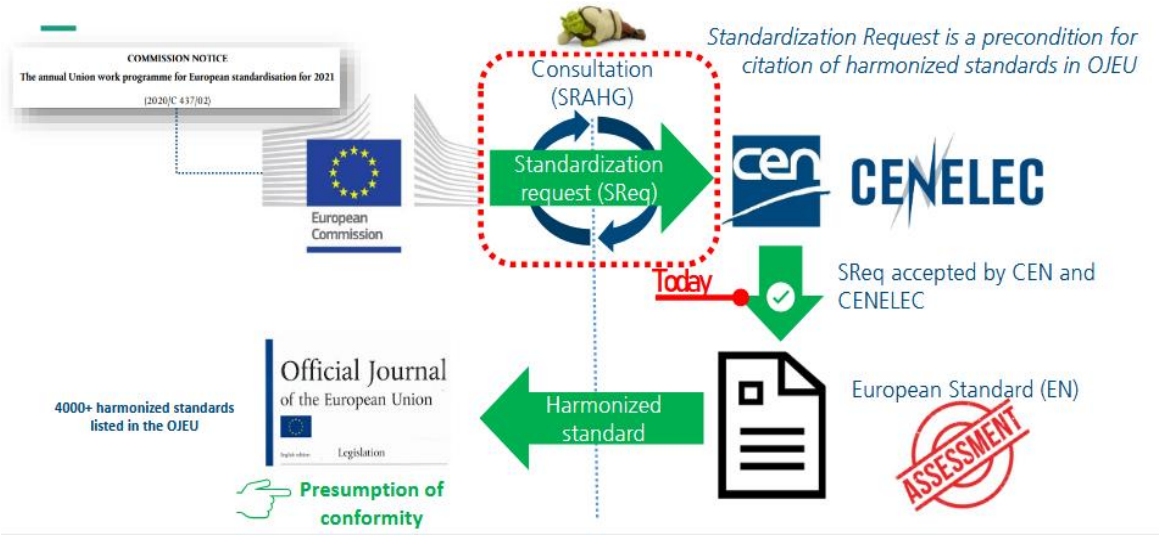

Figure 6 : Regulatory and standardization framework (Source : Technische Universitat Wien, 2024).

[39] ITU, https://www.itu.int/fr/ITU-T/publications/pages/recs.aspx.

a) Les principales normes CEN/CENELEC

Un rapprochement CEN et CENELEC a été fait afin de renforcer la coopération entre les deux organismes de normalisation, mais chacune de ces deux organisations dispose de ses propres prérogatives. CEN est chargée de l'élaboration et de la publication des normes européennes pour tous les secteurs sauf l'électrotechnique et les télécoms qui sont la prérogative du CENELEC.

Réunissant une pluralité d'acteurs industriels, consommateurs, administratifs et des experts nationaux, ces normes sont développées de manière consensuelle, transparente et ouverte.

Les normes CEN/CENELEC (EN) sont à destination des membres européens dans la mesure où 30 % d'entre elles sont développées à la demande de la Commission européenne. Ceci explique qu'après la publication d'une norme européenne, les normes nationales en conflit avec la nouvelle norme européenne doivent être modifiées. Ainsi, une norme européenne devient la norme nationale dans l'ensemble des 34 pays membres du CEN et/ou du CENELEC[40]. Parmi les normes mises en place[41] :

Sécurité incendie

- EN 54 (*Fire detection and fire alarm systems*) : exigences pour les systèmes de détection et d'alarme incendie.
- EN 2 : définition des catégories de feux.
- EN 3 : exigences de conception, de performance, de test et de marquage des extincteurs portatifs.

Cybersécurité et IOT

- EN 17927 (*Security Evaluation Standard for IoT Platforms – SESIP*) : méthodologie d'évaluation de cybersécurité pour plateformes IoT.

Services professionnels

- EN 16114 (*Management consultancy services Standard*) : encadrement des services de conseil en management.

[40] Cenelec, European standardization,https://www.cencenelec.eu/european-standardization/.
[41] Wikipédia, Comité européen de normalisation en électronique et en électrotechnique, 2026,https://fr.wikipedia.org/wiki/Comit%C3%A9_europ%C3%A9en_de_normalisation_en_%C3%A9lectronique_et_en_%C3%A9lectrotechnique.

Sécurité des produits

- N 71 : série portant sur la sécurité des jouets.
- EN 71-1 : propriétés mécaniques et physiques.
- EN 71-2 : inflammabilité.
- EN 71-3 : migration de certains éléments chimiques (plomb, cadmium…), etc.

b) Les JTC émanant des CEN et CENELEC

i. JTC13

Crée en 2017, le JTC13 joue depuis un rôle central dans la normalisation de la cybersécurité européenne regroupant plus de 150 experts européens issus de la cybersécurité et de la protection des données.

Les transpositions du JTC13 des principales normes ISO/IEC du SC27

EN ISO/IEC 15408-1	Critères communs	
EN ISO/IEC 15408-2		
EN ISO/IEC 15408-3		
EN ISO/IEC 15408-4		
EN ISO/IEC 15408-5		
EN ISO/IEC 18045	Evaluation method for common criteria	
EN ISO/IEC 19608		
EN ISO/IEC 19790		
EN ISO/IEC 24760-1		
EN ISO/IEC 24760-2		
EN ISO/IEC 24760-3		
EN ISO/IEC 27000:2017	270XX series	
EN ISO/IEC 27001:2017		
EN ISO/IEC 27002:2017		
EN ISO/IEC 27006		
EN ISO/IEC 27007		
EN ISO/IEC 27010		
EN ISO/IEC 27011		

EN ISO/IEC 27017	270XX series	
EN ISO/IEC 27018:2014		
EN ISO/IEC 27019:2017		
EN ISO/IEC 27037:2016		
EN ISO/IEC 27038:2016		
EN ISO/IEC 27041:2016		
EN ISO/IEC 27042:2016		
EN ISO/IEC 27043:2016		
EN ISO/IEC 29100		
EN ISO/IEC 29101		
EN ISO/IEC 29134:2020		
EN ISO/IEC 29147		
EN ISO/IEC 29151		
EN ISO/IEC 27701		
EN ISO/IEC 30111:2013		
EN ISO/IEC 19896-1		
EN ISO/IEC 19896-2		
EN ISO/IEC 19896-3		
EN ISO/IEC DTS 23532-1		
EN ISO/IEC DTS 23532-2		
EN ISO/IEC 27033-1		
EN ISO/IEC 27033-2		
EN ISO/IEC 27033-3		
EN ISO/IEC 27033-4		
EN ISO/IEC 27033-5		
EN ISO/IEC 27033-6		
EN ISO/IEC 27033-7		
EN ISO/IEC 27036-1		
EN ISO/IEC 27036-2		
EN ISO/IEC 27036-3		
EN ISO/IEC 27036-4		
EN ISO/IEC 21878		
EN ISO/IEC 27039		

Les normes spécifiques développées par le JTC13

EN 17529	Data protection and privacy by design and by default	JTC13 WG5
EN 17640	Fixed-time cybersecurity evaluation methodology for ICT products	JTC13 WG3
EUCS1	Multi-layered approach for a set of information security and cybersecurity requirements for cloud services	Standard pour soutenir le schéma de certification EUCS
EUCS2	Requirements for Conformity Assessment Bodies certifying Cloud Services	Standard pour soutenir le schéma de certification EUCS
	Guidelines on a sectoral cyber security assessment	JTC13 WG3
EN 17927	Security Evaluation Standard for IoT Platforms (SESIP).	JTC13 WG3
EN 18031-1/2/3	Exigences communes en matière de sécurité applicables aux équipements radioélectriques conformément à l'article 3.3, points d), e) et f) de l'acte délégué de la directive RED.	JTC13 WG8
EN17740	Requirements for professional Profiles related to Personal Data Processing and Protection	JTC13 WG5
EN 17799	Personal Data Protection Requirements for Processing Operations	JTC13 WG5
CEN/CLC/TS 17880	Protection Profile for Smart Meter - Minimum Security Requirements	JTC13 WG6

ii. JTC21

Créé en 2021, le JTC21 réunit 3000 experts de 20 pays. Ce comité chargé d'élaborer des normes européennes harmonisées, en lien avec l'intelligence artificielle, est notamment en alignement avec le règlement européen *AI act*. Ainsi, les entreprises qui respectent ces normes harmonisées bénéficieront d'une présomption légale de conformité avec les exigences de la loi sur l'IA[42].

Le comité élabore des normes à l'appui de la loi sur l'IA, concernant les sujets suivants[43] :

- Cadre de fiabilité de l'IA.
- Gestion des risques liés à l'IA : Régler les risques opérationnels.

[42] CENELEC, About the Joint Technical Committee | CEN-CENELEC JTC 21, 2024, https://jtc21.eu/about/.
[43] CENELEC, Artificial Intelligence, https://www.cencenelec.eu/areas-of-work/cen-cenelec-topics/artificial-intelligence/.

- Système de gestion de la qualité de l'IA : Assurer des processus solides pour le développement de l'IA.
- Évaluation de la conformité de l'IA : Faciliter la vérification de la conformité.

Le processus de normalisation suit plusieurs étapes : la Commission fait la demande de normalisation, puis les normes sont rédigées, et adoptées par consensus, enfin, ces mêmes normes sont ensuite publiées au Journal officiel de l'Union européenne (JOUE). Des normes plus spécifiques viendront ensuite compléter les normes dans les domaines suivants : les ensembles de données, le biais, la vision par ordinateur, la cybersécurité, la robustesse, l'enregistrement des armes et le traitement du langage naturel.

Le JTC 21 collabore avec les organisations internationales de normalisation ISO/CEI dans ou souci d'adaptation des normes mondiales aux besoins européens.

iii. JTC24 Digital Product Passport

Fondé en 2023, ce JTC est récent et a été créé dans le cadre d'une réglementation européenne plus large, dans le but de répondre à la demande de normalisation (SReq).
Ce contexte règlementaire est défini par le *European Green Deal* qui a pour ambition d'atteindre la neutralité climatique d'ici 2050, préserver la biodiversité, mettre en place une économie circulaire et éliminer la pollution, tout en renforçant la compétitivité de l'industrie européenne.

Ces normes harmonisées sont élaborées conformément :

- Au règlement sur l'écoconception des produits durables (ESPR) datant de 2022. Il vise à promouvoir la durabilité environnementale sur des produits conçus de sorte à être écologiques et circulaires.
- A la régulation des batteries électriques (2023). Il fournit un cadre juridique visant à promouvoir la durabilité, la circularité, la sécurité et la transparence.

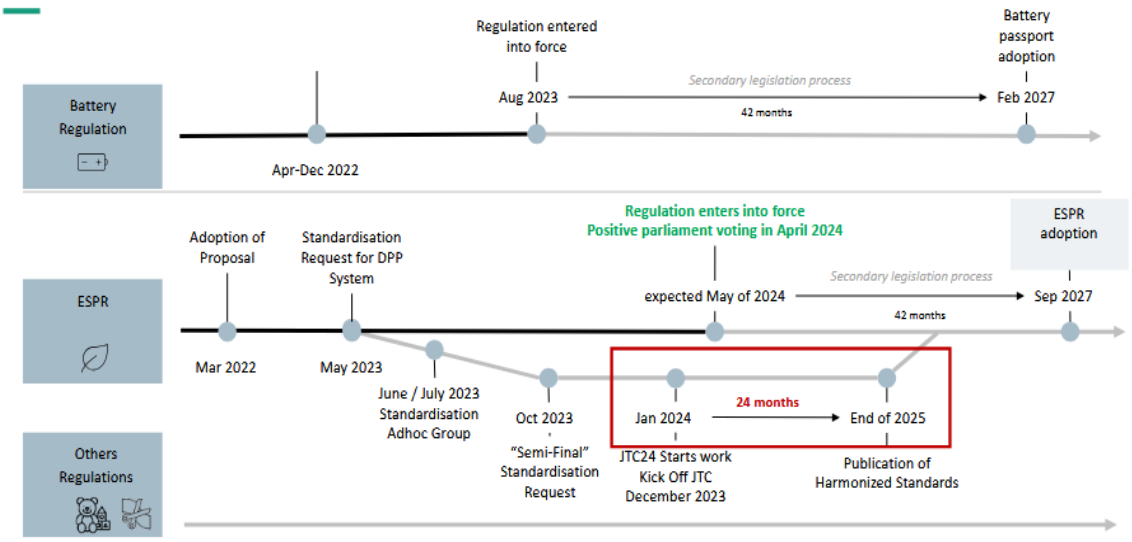

Figure 7 : JTC 24 – Digital Product Passport – Framework and system, T. Knothe, CEN CENELEC[44].

c) Les principales normes ETSI

L'ETSI est un organisme de normalisation reconnu au niveau européen dont les normes structurent les télécommunications modernes. Il a pour objectif d'élaborer des normes techniques pour les télécoms, les réseaux, les médias et les technologies de l'information. Deux classes de normes sont produites par l'ETSI :

- Normes européennes (EN) : obligatoires une fois adoptées par l'UE.
- Normes ETSI (ES) : normes volontaires, plus rapides à publier.

Bien que les normes soient à destination des entités économiques et politiques au sein de l'UE, ces normes disposent d'un **impact mondial**, dont les normes couvrant les domaines suivants : GSM, LTE, 5G.

Les principales normes ETSI dans le domaine de la sécurité

EN 303 645	Cyber Security for Consumer Internet of Things : Baseline Requirements	Transposition en EN de la TS 103 645
ETSI TR 103 305	Critical security controls	

[44] Thomas Knothe, JTC 24, 2024, https://bim4bipv.project.tuwien.ac.at/wp-content/uploads/2024/07/05-20240619-dpp-regulatory-and-standardization-framework-knt.pdf.

ETSI TS 103 523	Middlebox security protocols	Part 1-5
ETSI TR 103 621	Guide to cybersecurity of IOT	
ETSI TR 103 719	Guide to Identity Based Cryptography	
ETSI TR 103 787	Cybersecurity for SMEs	
ETSI TS 103 458	Application of Attribute-Based Encryption (ABE) for data protection on smart devices, cloud and mobile services	
ETSI TS 103 486	Identity Management and Discovery for IoT	
ETSI TS 173 532	Attribute Based Encryption for Attribute Based Access Control	
ETSI TS 103 645	Cyber Security for Consumer Internet of Things : Baseline Requirements	
ETSI TS 103 651	Critical Security Controls for MSP middlebox defence	
ETSI TS 103 701	Cyber security assessment for consumer IoT products	Evaluation method associée à la norme EN 303-645
ETSI TS 103 732	Consumer Mobile Device Protection Profile	
ETSI TS 103 994	Privileged Access Workstations	
ETSI TS 104 010	Security Evaluation Standard for IoT Platforms (SESIP) Profile for Secure Consumer IoT Devices	
ETSI TS 119 312	Electronic Signatures and Infrastructures (ESI) ; Cryptographic Suites	
ETSI TS 119 461	Policy and security requirements for trust service components providing identity proofing of trust service subjects	

d) Les normes harmonisées dans le cadre du Cyber Resilience Act (CRA)

Le 3 février 2025, la Commission européenne a publié une décision d'exécution visant à soutenir la mise en conformité des produits avec les exigences essentielles de cybersécurité du CRA. Ces normes horizontales et verticales ont été réparties entre le CEN, CENELEC et l'ETSI. La finalisation de ces travaux normatifs est prévue sur 2026 et 2027. Une fois citées au JOUE, ces normes harmonisées permettront aux industriels de bénéficier d'une présomption de conformité aux exigences essentielles du CRA, notamment pour les produits « importants » de classe 1.

Conclusion

Le point de vue de Jean-Pierre Quemard,

CEO de KAT

La standardisation : un enjeu de souveraineté ?

La standardisation internationale n'est plus seulement un enjeu de sureté du consommateur, d'interopérabilité technique ou de certification de produits mais elle accompagne la transition numérique et verte dans tous les domaines : IA, ordinateurs quantiques, passeport des produits, cybersécurité, bio technologies, cycle de vie des produits, etc.

C'est aussi pour l'Europe une occasion unique de protéger nos valeurs face à une course globale dominée par les USA et la Chine.

Il s'agit de bâtir un système qui protège les intérêts géopolitiques européens, défend la compétitivité et renforce la cohésion du marché intérieur européen tout en préservant l'aspect international des normes. A ce titre la normalisation, en tant qu'outil de la souveraineté numérique, est un enjeu crucial pour L'Europe.

Remerciements

Ce document, réalisé par l'ACN, est le fruit d'un travail collectif, nourri par l'engagement et l'expertise de la commission NORSEC et des experts institutionnels.

Ainsi, l'Alliance pour la Confiance Numérique tient à adresser ses remerciements à l'ensemble de la commission NORSEC, et plus particulièrement aux contributeurs suivants :

- *ATOUI Roland (Red Alert Labs)*
- *FERAUD Alban (IN Groupe)*
- *QUEMARD Jean-Pierre (KAT)*
- *SCUTO Nicolas (ministère de l'Intérieur)*
- *SULZER Jean-François (ex-Thales)*
- *ZAMORA François (Orange)*

Un grand remerciement à l'équipe qui a élaboré ce document :

- *Jenifer Bitar*
- *Natasha Blanca*
- *Ilona Quette*

A propos du CSF IS

Le Comité Stratégique de la Filière Industrie de Sécurité (CSF IS) a été créé en 2018 sous l'égide du Conseil National de l'Industrie (CNI).

Le CSF IS constitue une plateforme d'échanges public/privé pour la filière française de la sécurité, incluant les industriels, les institutions, les collectivités, les organisations syndicales dont l'ACN, les pôles de compétitivité et les acteurs publics, afin d'engager un dialogue concret entre l'Industrie et l'Etat pour répondre aux enjeux de souveraineté, de résilience et de compétitivité de notre pays.

Les travaux du CSF se développent dans le cadre de contrats de filière. Le premier contrat (2020-2023) a été notamment rythmé par le défi de sécurisation des Jeux Olympiques de Paris 2024 qui a permis le développement de solutions innovantes de la filière et a mis en avant une collaboration étroite entre l'Etat et les industries. Les axes majeurs du nouveau contrat (2024-2026) s'articulent autour du renforcement du dialogue stratégique avec l'Etat, le soutien aux PME et l'adaptation de la filière aux évolutions règlementaires (directives REC ou NIS 2).

A propos de la Commission NORSEC

La Commission NORSEC du CSF IS est une instance informelle qui permet de rassembler l'ensemble des experts et participants aux différents groupes/comités de normalisation français et européens. L'objectif est de partager les informations sur les travaux en cours dans ces différentes instances, afin de créer une meilleure compréhension commune et de permettre une analyse éclairée sur ces enjeux stratégiques.

La commission NORSEC est actuellement animée par l'ACN et présidée par Roland Atoui (Red Alert Labs). Elle est constituée d'industriels de l'ensemble des groupements participant au CSF, de représentants des instances de normalisation et des pouvoirs publics.

A propos de l'ACN

L'Alliance pour la Confiance Numérique (ACN) est le syndicat professionnel qui représente les entreprises (leaders mondiaux, PME/TPE, et ETI) du secteur de la confiance numérique et notamment celles de l'identité numérique, de la cybersécurité, l'IA de confiance et de la blockchain.

La France dispose dans ce domaine d'un tissu industriel très performant et d'une excellence internationalement reconnue grâce à des leaders mondiaux, des PME, des ETI et aux différents acteurs dynamiques du secteur. On dénombre 2 178 entreprises réalisant en France 19 milliards d'euros de chiffre d'affaires dans ce secteur en forte croissance (8% de croissance annuelle moyenne depuis 2016). Les 120 membres de l'Alliance pour la Confiance Numérique (ACN), dont 87% de PME/ TPE- ETI, représentent 2/3 du chiffre d'affaires des entreprises françaises de la Confiance Numérique dans le monde (fabricants de matériel, éditeurs de logiciels, intégrateurs, services, laboratoires d'évaluation de sécurité, recherche).

L'ACN est membre de la FIEEC (Fédération des Industries Electriques, Electroniques et de Communication), est membre associé du Campus cyber et participe activement aux travaux du CSF (Comité Stratégique de Filière) des Industries de Sécurité. Par ailleurs, l'ACN est également membre fondateur d'ECSO (*European CyberSecurity Organisation*). Retrouvez toutes les informations sur notre site web : https://www.confiance-numerique.fr/

Retrouvez nos publications :