|  |  |  |
| --- | --- | --- |
| itu_logo | **Assemblée mondiale de normalisation des télécommunications (AMNT-16)Hammamet, 25 octobre - 3 novembre 2016** | CCITT/ITU-T 60th Anniversary logo |
|  |  |
|  |  |
| **SÉANCE PLÉNIÈRE** | **Révision 1 duDocument 58-F** |
|  | **27 octobre 2016** |
|  | **Original: anglais** |
|  |
| Directeur du TSB |
| Conclusions du troisième Colloque mondial sur la normalisation |
|  |
|  |

|  |  |
| --- | --- |
| **Résumé:** | On trouvera dans le présent rapport un résumé des conclusions du troisième Colloque mondial sur la normalisation (GSS). La Révision 1 de ce document comprend un résumé de toutes les présentations faites au GSS (Appendice 1). |

Conclusions du troisième Colloque mondial sur la normalisation

La troisième édition du Colloque mondial sur la normalisation, qui s'est tenu à Hammamet (Tunisie) le 24 octobre 2016, a rassemblé des responsables de renom des milieux de la normalisation pour discuter de la manière d'intégrer au mieux les questions liées à la sécurité, à la vie privée et à la confiance dans les activités de normalisation.

# 1 Introduction

Les Colloques mondiaux sur la normalisation (GSS) sont l'occasion d'avoir des débats de haut niveau sur les politiques en matière de normalisation et de réfléchir à l'évolution et à la dynamique du secteur des technologies de l'information et de la communication (TIC), ainsi qu'aux conséquences qui en découlent pour l'élaboration des normes techniques. Le GSS se tient avant le début de l'Assemblée mondiale de normalisation des télécommunications (AMNT) de l'UIT, qui a lieu tous les quatre ans. Les éditions précédentes du GSS se sont déroulées à Johannesburg en 2008 et à Dubaï en 2012.

Le thème du GSS-12, à savoir *La normalisation et les points communs entre le secteur des TIC et d'autres secteurs comme les soins de santé, les services collectifs et les transports*, s'est avéré être tout à fait d'actualité et les conclusions du Colloque ont donné des orientations précieuses pour les travaux de normalisation menés à l'UIT pendant la période d'études 2013-2016. Les participants au GSS-12 ont abordé des questions liées à la sécurité, à la vie privée et à la confiance dans les infrastructures et les services TIC, notamment dans le cadre des débats sur la transmission sans fil de données médicales, le stockage de données relatives aux déplacements des véhicules connectés et la collecte par les détaillants en ligne des données relatives aux consommateurs. Dans ces secteurs, il est nécessaire d'élaborer des cadres normalisés pour avoir l'assurance qu'un service est doté d'attributs de sécurité fiables et que les besoins des utilisateurs relatifs à la sécurité et à la vie privée sont pris en compte.

Les participants au GSS-16 se sont interrogés sur la manière dont les parties prenantes concernées pourraient collaborer pour élaborer des cadres internationaux relatifs à la sécurité, à la vie privée et à la confiance. Le Colloque a rassemblé des spécialistes de renom dans les domaines de la sécurité, de la vie privée et de la confiance dans le secteur des TIC, qui représentaient des gouvernements, des régulateurs, des organismes de normalisation et le secteur privé. Les participants au Colloque ont fait part de leurs points de vue sur les éléments de ces cadres, qui, à leur sens, sont essentiels ainsi que sur ceux de ces éléments qui devraient occuper une place prioritaire dans les travaux de normalisation de l'UIT qui seront menés pendant la période d'études 2017-2020.

**S. E. M. Mohamed Anouar Maarouf**, Ministre des technologies de communication et de l'économie numérique, Tunisie, a prononcé une allocution de bienvenue. **M.** **Houlin Zhao**, Secrétaire général de l'UIT, et **M. Chaesub Lee**, Directeur du Bureau de la normalisation des télécommunications, ont prononcé des remarques liminaires. Le Colloque était présidé par **M. Mongi Marzoug**, ancien Ministre des TIC de la Tunisie.

La séance d'ouverture du GSS-16 a été suivie de trois sessions consacrées au thème du Colloque abordé sous l'angle de la réglementation et des politiques, du secteur privé et de la normalisation. La Section 2 du présent rapport du GSS est un examen du thème du Colloque dans le contexte du système des Nations Unies, et la Section 3 est un résumé des principales conclusions et recommandations de chaque session du Colloque. On trouvera dans l'Appendice I du présent document un résumé détaillé de tous les débats du GSS-16.

Le programme définitif, ainsi que les biographies des intervenants et les exposés sont disponibles à l'adresse: <http://itu.int/en/ITU-T/wtsa16/gss/>.

Conformément à la Résolution 122 (Rév. Guadalajara, 2010) de la Conférence de plénipotentiaires et à la Résolution 1272 (MOD) du Conseil de l'UIT, les conclusions du GSS-16 détaillées dans le présent rapport sont soumises pour examen à l'AMNT-16.

# 2 Sécurité, vie privée et confiance dans le secteur des TIC – le contexte des Nations Unies

Grâce aux TIC, des milliards de personnes peuvent échanger des informations numériques dans le monde entier. L'utilisation de ces technologies, qui s'appuie essentiellement sur des normes techniques, a soulevé un grand nombre de problèmes liés à la confidentialité et à la sécurité des communications, et, en définitive, à la confiance des utilisateurs finals dans les TIC.

L'UIT s'attaque à ces problèmes, en tant qu'organisation de normalisation qui a pour objectif d'élaborer des normes, d'application volontaire, sur une utilisation des TIC respectueuse de la vie privée[[1]](#endnote-1), et en tant qu'organisation intergouvernementale qui a pour mission d'instaurer la confiance et la sécurité dans l'utilisation des TIC[[2]](#endnote-2). Le Sommet mondial sur la société de l'information a désigné l'UIT comme coordonnateur pour la grande orientation C5, afin de collaborer avec les Etats Membres de l'UIT et les autres parties prenantes, en vue de "*[r]enforcer le cadre de sécurité et de confiance en adoptant des initiatives complémentaires et synergiques dans les domaines de la sécurisation de l'utilisation des TIC, ainsi que des initiatives ou des lignes directrices relatives au droit à la confidentialité, à la protection des données et à la protection des consommateurs*".

Les normes internationales de base relatives à la protection de la vie privée figurent avant tout dans les traités sur les droits de l'homme, par exemple la Déclaration universelle des droits de l'homme de 1948[[3]](#endnote-3) et le Pacte relatif aux droits civils et politiques de 1966[[4]](#endnote-4) des Nations Unies qui contiennent tous les deux des dispositions sur le droit à la protection de la vie privée (articles 12 et 17 respectivement). Toutefois, ces traités ne mentionnent pas expressément le traitement numérique des informations personnelles, une thématique qui, dans le contexte du système des Nations Unies, n'a été prise en considération que sous la forme d'un document d'orientation non contraignant, à savoir les Principes directeurs des Nations Unies pour l'utilisation des fichiers personnels informatisés de 1990[[5]](#endnote-5).

Plusieurs conventions internationales juridiquement contraignantes prévoient certes un droit au respect de la vie privée, par exemple la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel[[6]](#endnote-6), la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales[[7]](#endnote-7) et la Convention américaine relative aux droits de l'homme[[8]](#endnote-8), mais ces instruments juridiques ont été élaborés et adoptés au niveau régional et non mondial. Bon nombre de ces accords régionaux s'appuient sur les mêmes principes fondamentaux relatifs à la vie privée, tels que la notion de consentement éclairé de la personne et l'efficacité des mesures de sécurité mises en place avant le traitement des informations personnelles[[9]](#endnote-9).

Plusieurs parties prenantes ont demandé qu'une plus grande attention soit accordée à la nécessité de définir une approche commune universelle pour le traitement des informations personnelles. A titre d'exemple, dans le cadre de leur Conférence internationale, les Commissaires à la protection des données et de la vie privée ont appelé: a) les Nations Unies à élaborer une "*Convention universelle* *pour la protection des personnes à l’égard du traitement automatisé des données à caractère personnel*"juridiquement contraignante; b) les organisations internationales "*à s'engager à se conformer à des principes compatibles avec les principaux instruments qui touchent à la protection des données et à la vie privée*"; et c) les fabricants de matériel informatique et de logiciel "*à développer des produits et des systèmes intégrant des technologies respectueuses de la vie privée*"[[10]](#endnote-10)*.*

A sa 68ème session (2013), l'Assemblée générale des Nations Unies a répondu à cet appel en adoptant une Résolution intitulée "*Le droit à la vie privée à l'ère du numérique*", dans laquelle tous les Etats Membres des Nations Unies sont invités "*à respecter et à protéger le droit à la vie privée, notamment dans le contexte de la communication numérique*"[[11]](#endnote-11). En application de cette Résolution, le Conseil des droits de l'homme de l'Organisation des Nations Unies a nommé un Rapporteur spécial chargé, en particulier, de faire rapport sur des violations présumées du droit à la vie privée, notamment concernant les problèmes liés à l'utilisation des nouvelles technologies.

# 3 Principales conclusions du GSS-16

## 3.1 Principes réglementaires pour la sécurité, la vie privée et la confiance

*Rappelant que le respect de la vie privée et la protection des données sont des valeurs fondamentales pour les personnes et les sociétés, et que la Déclaration universelle des droits de l'homme consacre le respect de la vie privée comme un droit fondamental;*

*Notant qu'aujourd'hui, nous sommes tributaires, dans presque tous les aspects de notre vie quotidienne, des infrastructures et des services TIC et, par conséquent, nous serions touchés si la fiabilité de ces infrastructures et de ces services ne pouvait être assurée; et*

*Reconnaissant que les violations de données et les incidents de sécurité constituent une tendance inquiétante, qui a des répercussions négatives sur la confiance.*

*Les participants du GSS ont souligné combien il est important:*

– de tirer parti des **cadres internationaux** qui définissent les principes fondamentaux de sécurité, de respect de la vie privée et de confiance, et de mettre en place des mécanismes pour mettre en oeuvre ces principes;

– de promouvoir l'adhésion aux **principes de protection de la vie privée dès la conception, l'évaluation des incidences sur la protection de la vie privée et l'élaboration de** **technologies renforçant la protection de la vie privée** (PET), technologies qui, lorsqu'elles sont intégrées aux infrastructures et services TIC, limitent au maximum le traitement des informations d'identification personnelle;

– de mettre en place des moyens permettant un échange d'informations **entre les secteurs public et privé** concernant les menaces qui pèsent sur les infrastructures et les services TIC, les bonnes pratiques et les stratégies d'atténuation;

– de mobiliser la communauté internationale et de nouer des partenariats afin **de donner aux pays davantage de moyens** pour se protéger en cas de cyberattaques, ce qui renforcera leur capacité à détecter les incidents de sécurité et à réagir de façon coordonnée à de tels incidents;

– de trouver un juste équilibre entre la nécessité de protéger la vie privée des personnes et la nécessité de promouvoir une **utilisation innovante des données** au service de l'économie numérique. Lorsqu'elles sont intégrées dans les nouvelles technologies et les nouveaux services, les bonnes pratiques en matière de protection de la vie privée et de sécurité sont un excellent argument de vente auprès des clients et contribuent à améliorer le réseau dans son ensemble;

– de contribuer à l'élaboration de **normes internationales pour faire face aux problèmes de portée mondiale**, conscients du fait que les cyberattaques ignorent les frontières nationales, que les atteintes au respect de la vie privée et à la sécurité sapent la confiance dans les TIC, et que des cadres de sécurité normalisés à l'échelle internationale sont nécessaires pour donner l'assurance que les attributs de sécurité d'un service sont fiables et que les exigences d'un utilisateur quant à sa sécurité et au respect de sa vie privée sont respectées au-delà des frontières;

– de promouvoir l'élaboration de **normes pour la "désidentification" des données personnelles** et la **portabilité des données**, normes propres à améliorer la protection des consommateurs et à donner plus de latitude aux consommateurs pour souscrire ou résilier un abonnement à des services TIC.

## 3.2 Comment le secteur privé répond aux attentes des utilisateurs finals en matière de sécurité, de vie privée et de confiance

*Réaffirmant que les technologies de l'information et de la communication et de la numérisation offrent des possibilités immenses pour améliorer la vie des personnes et la société;*

*Reconnaissant que les failles de sécurité, les violations de la vie privée et le manque de confiance dans les infrastructures et les services TIC peuvent gravement menacer l'activité et la réputation d'une entreprise; et*

*Appelant de leurs voeux l'adoption de normes internationales susceptibles d'être appliquées,*

*Les participants du GSS ont souligné combien il est important:*

– d'appuyer et de promouvoir les principes de **transparence** et **d'intégrité technologique**. Puisqu'il ne peut y avoir de confiance sans transparence, les utilisateurs devraient pouvoir savoir comment leurs données sont utilisées et décider d'accepter ou non une telle utilisation. L'intégrité technologique va de pair avec la nécessité d'une sécurité renforcée dans les infrastructures et les services TIC; elle appelle des mesures de protection de la vie privée et vise à écarter toute possibilité de fonctionnalités cachées, afin de prévenir toute modification non autorisée des informations et d'instaurer la confiance quant à l'exactitude, l'exhaustivité et la fiabilité des informations;

– d'atténuer les risques que posent les **botnets de l'Internet des objets** (IoT) en ayant recours à des normes de sécurité. Les cas signalés d'utilisation abusive de dispositifs IoT dans des attaques massives par déni de service (DDoS) sont en augmentation. Ces attaques peuvent conduire à des violations des données et nuire considérablement à l'activité économique et à la réputation des organisations touchées. Il faut étudier comment on peut tirer parti des progrès réalisés dans des domaines comme la cryptographie légère ainsi que des méthodes de sécurité normalisées pour atteindre des niveaux de sécurité élevés avec une puissance de calcul limitée;

– d'évaluer les incidences de **l'informatique quantique** sur la sécurité, la vie privée et la confiance et étudier les **technologies capables de résister à une attaque quantique**. Bien que l'informatique quantique n'en soit qu'à ses débuts, il est communément admis qu'une fois que cette technologie pourra concrètement être utilisée, les méthodes de chiffrement classiques, qui aujourd'hui protègent les paiements en ligne, les opérations bancaires, les conversations électroniques et téléphoniques, pourraient rapidement devenir obsolètes. Le moment est venu d'évaluer les incidences de l'informatique quantique et de faire des recherches, de procéder à des tests, d'élaborer des normes et de se préparer pour opérer une transition vers de nouveaux systèmes de sécurité résistant aux attaques quantiques, et ce bien avant que nos systèmes ne deviennent vulnérables à de telles attaques.

## 3.3 Approche des organismes de normalisation concernant la sécurité, la vie privée et la confiance

*Reconnaissant le rôle crucial que jouent les normes dans la sécurité, la protection de la vie privée et l'instauration de la confiance dans les infrastructures et les services TIC;*

*Soulignant que la sécurité, la vie privée et la confiance sont des sujets d'étude reconnus dans nombre d'organismes internationaux de normalisation qui s'intéressent aux TIC et à d'autres domaines de la technologie; et*

*Préconisant l'élaboration de normes pour répondre aux problèmes liés à la sécurité, la vie privée et la confiance,*

*Les participants du GSS ont souligné combien il est important:*

– d'appuyer une approche de **protection de la vie privée dès la conception**, en tenant dûment compte des considérations liées au respect de la vie privée tout au long du processus d'élaboration des normes. Cette approche peut être étayée par des normes qui intègrent des caractéristiques de protection de la vie privée et de protection des données; les normes peuvent aussi se révéler efficaces pour assurer l'interopérabilité des caractéristiques de protection de la vie privée;

– de comprendre le rôle des **logiciels à code source ouvert** dans les réponses à apporter aux problèmes de sécurité, de respect de la vie privée et de confiance. Les logiciels à code source ouvert et les normes contribuent de façon complémentaire à la croissance et l'innovation dans le secteur des TIC. Les logiciels sont de plus en plus complexes et, bien que les communautés open source et les communautés de normalisation collaborent déjà dans de nombreux domaines, il convient de redoubler d'efforts afin de faciliter les échanges de travaux entre ces communautés et, par là même, garantir une mise en oeuvre des logiciels avec des niveaux élevés de qualité et de sécurité;

– de **renforcer la collaboration** entre les organismes de normalisation en ce qui concerne l'élaboration de cadres internationaux pour la sécurité, la vie privée et la confiance, en reconnaissant leurs forces et leurs mandats respectifs et en tirant parti des travaux en cours. Les organismes de normalisation devraient respecter les principes suivants: respect de la régularité des procédures, large consensus, transparence, équilibre et ouverture du processus de normalisation; importance attachée au bien-fondé sur le plan technique; interopérabilité; concurrence et innovation, dans l'intérêt de tous; mise à disposition des normes pour tous; enfin, adoption volontaire des normes. Les organismes de normalisation devraient également unir leurs efforts pour réduire les disparités entre les pays en développement et les pays développés en matière d'accès, mettre en place des normes et des cadres traitant de la sécurité, de la vie privée et de la confiance dans les infrastructures et les services TIC, et participer à leur élaboration sur un pied d'égalité.

Appendice I

Résumé détaillé des débats du GSS-16

(Le présent Appendice ne fait pas partie intégrante du présent Rapport.)

Session 1: Allocutions de bienvenue et discours-programmes

**S. E. Mohamed Anouar Maarouf**,Ministre des technologies de communication et de l'économie numérique, Tunisie [[Biographie](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Maarouf)] a souhaité la bienvenue à tous les participants et a remercié les membres de l'UIT d'avoir choisi Hammamet (Tunisie) pour tenir le Colloque mondial sur la normalisation (GSS) et l'Assemblée mondiale de normalisation des télécommunications (AMNT). Il a souligné la nécessité d'instaurer la confiance dans les infrastructures et les services TIC et reconnu l'importance du thème du GSS-16: *Sécurité, respect de la vie privée, confiance et normalisation*.

Dans ses remarques liminaires, **M. Mongi Marzoug** (ancien Ministre des TIC, Tunisie) [[Biographie](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Marzoug)], Président du Colloque, a souhaité la bienvenue en Tunisie à tous les participants ainsi qu'un agréable séjour à Hammamet. Il a souligné le rôle de la Tunisie dans l'édification de la société de l'information et décrit le rôle essentiel que jouent aujourd'hui les technologies de l'information et de la communication (TIC) dans notre vie quotidienne et l'importance qu'elles continueront d'avoir à l'avenir. Il a également rappelé que disposer de services TIC ouverts, sûrs, sécurisés et fiables dans tous les domaines (par exemple, la santé, la finance, les services d'utilité publique ou l'Internet des objets (IoT)) était essentiel au développement mondial. Dans ce contexte, il a fait observer que la normalisation avait un rôle majeur à jouer afin d'améliorer la sécurité des TIC, de protéger la vie privée et d'instaurer la confiance des particuliers, des gouvernements et des entreprises dans les services de TIC. Il a souligné que l'objectif de ce troisième Colloque était de présenter et d'examiner les contributions en matière de sécurité, de vie privée et de confiance dans les infrastructures et les services TIC de trois principales parties prenantes, à savoir le gouvernement et les régulateurs, les entreprises et les organismes de normalisation, mais aussi de soumettre des conclusions et des recommandations sur ces sujets à l'AMNT-16.

**M. Houlin Zhao** (Secrétaire général de l'UIT) [[Biographie](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Zhao)] a remercié la Tunisie, qui accueille le GSS et l'AMNT, pour l'appui fourni aux travaux de l'UIT. Il a décrit les retombées positives qu'avaient eues les éditions précédentes du GSS et expliqué en quoi le Colloque fournit un cadre international d'examen des politiques en matière de normalisation, rassemblant des dirigeants des secteurs public et privé qui se penchent sur la manière dont il convient d'utiliser la normalisation technique pour traiter les priorités changeantes du secteur des TIC. Les conclusions et les recommandations des éditions de 2008 et de 2012 du GSS sont toutes devenues des éléments essentiels du programme de travail de l'UIT dans le domaine de la normalisation. M. Zhao a également fait remarquer qu'avec un environnement des TIC sûr, les utilisateurs et les entreprises auront suffisamment confiance pour exploiter pleinement les possibilités offertes par les TIC, et que c'est en grande partie grâce à ses activités de normalisation que l'Union parvient à mener à bien sa mission qui est "d'instaurer la confiance et la sécurité dans l'utilisation des TIC". En conclusion, il a adressé ses remerciements à tous les orateurs, modérateurs et participants pour leur contribution au GSS-16.

Dans son allocution d'ouverture, **M. Chaesub Lee** (Directeur du Bureau de la normalisation des télécommunications de l'UIT) [[Biographie](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Lee)] a expliqué que les réseaux futurs devront pouvoir fournir un volume considérable d'applications TIC ainsi qu'un très large éventail de services. Les milliards de dispositifs et d'objets connectés permettront aux systèmes de communiquer et de tirer parti les uns des autres, en créant des écosystèmes intelligents capables d'adapter leur comportement pour être plus efficaces. Parmi les communications de prochaine génération, de nouvelles applications verront le jour, dans des domaines allant des services vocaux et vidéo à la robotique industrielle, en passant par les systèmes de transport intelligents, les opérations chirurgicales à distance, la réalité virtuelle et bien d'autres. M. Lee a indiqué que cette tendance croissante au perfectionnement des TIC ainsi que leur omniprésence sans précédent appellaient des changements profonds dans les infrastructures de réseau et les services. Alors que les sociétés évoluent vers un monde où presque tous les aspects de l'activité économique et sociale dépendront des TIC, il devient essentiel de créer des infrastructures et des services des TIC dignes de notre confiance. M. Lee a souligné le rôle des normes techniques pour prévenir l'apparition de "silos" de données dans différents secteurs de nos économies et a fait observer que les spécialistes participant aux activités de normalisation de l'UIT travaillent pour appuyer la mise en place d'un écosystème partagé et intégré pour les données.

Session 2: Principes réglementaires pour la sécurité, la vie privée et la confiance

Le modérateur de cette session, lors de laquelle des principes réglementaires pour la sécurité, la vie privée et la confiance ont été établis, était **M. Bilel Jamoussi** (Chef du Département des commissions d'études du Bureau de la normalisation des télécommunications de l'UIT) [[Biographie](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Jamoussi)].

Dans son discours liminaire, **M. John Edwards** (Commissaire à la protection des données et de la vie privée en Nouvelle-Zélande et Président du Comité exécutif de la Conférence internationale des commissaires à la protection des données et de la vie privée) [[Biographie](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Edwards)] a reconnu qu'il existait une évolution progressive mais de plus en plus marquée vers l'obtention de consensus entre des organisations auparavant distinctes et que toutes s'accordent à dire que la protection de la vie privée est en passe de devenir l'une des questions déterminantes de notre époque. M. Edwards a rappelé qu'à sa 68ème session (2013), l'Assemblée générale des Nations Unies a adopté une Résolution intitulée "*Le droit à la vie privée à l'ère du numérique*", dans laquelle tous les Etats Membres des Nations Unies sont invités "*à respecter et à protéger le droit à la vie privée, notamment dans le contexte de la communication numérique*". Il a présenté les travaux de l'organisation qu'il représente, à savoir la Conférence internationale des commissaires à la protection des données et de la vie privée (ICDPPC), et proposé plusieurs pistes pour renforcer la confiance en appliquant des principes de protection de la vie privée et, éventuellement, en élaborant des normes pour le secteur des télécommunications, notamment:

– promouvoir l'adhésion aux principes de protection de la vie privée dès la conception, l'évaluation des incidences sur la protection de la vie privée et l'élaboration de technologies renforçant la protection de la vie privée;

– veiller à ce que seuls les représentants de l'Etat légalement habilités aient accès aux réseaux, systèmes, contenus, communications et métadonnées, et ce uniquement dans les cas où cet accès est nécessaire et proportionné;

– promouvoir la transparence en ce qui concerne l'accès aux données personnelles et leur utilisation à des fins autres que celles pour lesquelles le sujet des données a donné son consentement;

– élaborer et promouvoir des normes et des sauvegardes appropriées pour permettre la "désidentification" des données personnelles et empêcher le rétablissement de l'identification de particuliers à partir d'ensembles de données anonymisées;

– élaborer des normes pour la portabilité des données, permettant de contribuer à améliorer la protection des consommateurs et à donner plus de latitude aux consommateurs pour souscrire ou résilier un abonnement à des services TIC;

– veiller à ce que les citoyens et les consommateurs continuent à savoir, de manière transparente, sur quelles bases les décisions automatiques les concernant ont été prises.

Dans son intervention, **M. Victor Manuel Martinez Vanegas** (Directeur chargé des politiques internationales à l'Institut fédéral des télécommunications, Mexique) [[Biographie](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Vanegas)/[Présentation](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/GSS_IFT_Draft_Presentation.pdf)] a abordé le thème du Colloque selon une perspective globale, et a présenté les initiatives mises en oeuvre au niveau régional ainsi que le contexte national dans le domaine de la sécurité, de la vie privée et de la confiance dans les TIC.

Il a souligné les incidences positives du développement et de l'adoption des TIC sur la croissance économique et sociale, mais a mentionné qu'il existait également des menaces et des problèmes susceptibles de compromettre ces avantages. La sécurité, la vie privée et la confiance sont devenus des sujets de préoccupation importants qui doivent être traités de manière appropriée. A ce sujet, il a fait référence à des publications, déclarations et accords émanant notamment de l'Assemblée générale des Nations Unies, aux activités de normalisation de l'UIT-T et de la Commission électrotechnique internationale (CEI), ainsi qu'au Rapport 2015 sur l'économie de l'information de la Conférence des Nations Unies sur le commerce et le développement (CNUCED), dans lequel il est indiqué que "La sécurité et la confiance sont essentielles à la création d'un environnement favorable au commerce électronique". M. Martinez Vanegas a fait savoir que le nombre d'internautes de sa région, l'Amérique latine et les Caraïbes, connaissait la croissance la plus rapide au monde, et que répondre aux préoccupations liées à la sécurité, à la vie privée et à la confiance dans les TIC était nécessaire au développement économique et social de la région. Il a également souligné que les enseignements tirés dans la région ont démontré qu'aucun pays ne saurait assurer seul la sécurité de ses réseaux, et que la coopération revêtait un caractère essentiel.

**Ilias Chantzos** (Directeur principal, Affaires gouvernementales, EMEA, Conseiller mondial pour la protection des infrastructures essentielles et de la vie privée, Symantec, Etats-Unis) [[Biographie](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Chantzos)/[Document de référence](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/InternationalCyberNorms_Ch10%20-%20Symantec.pdf)] a fait observer que les facteurs politiques et réglementaires et les avancées technologiques avaient une influence réciproque. Il a évoqué le règlement général de l'UE sur la protection des données comme l'un des exemples les plus probants de cette dynamique. La directive sur la protection des données à caractère personnel en vigueur avait été adoptée plus de vingt ans auparavant et devait être considérablement modifiée afin de tenir compte de l'évolution, ou plutôt de la révolution, des technologies et d'autres éléments tels que les réseaux sociaux. Réciproquement, les technologies et les réseaux sociaux devront être utilisés selon les dispositions du nouveau règlement, qui est porteur de profonds changements quant à la manière dont les organismes publics et privés mettent en oeuvre la gouvernance des données, notamment en ce qui concerne la protection des données personnelles contre les cyberattaques. M. Chantzos a en outre présenté le concept d'intégrité technologique, qui va de pair avec la nécessité d'une sécurité renforcée dans les infrastructures et les services TIC; ce concept appelle des mesures de protection de la vie privée et vise à écarter toute possibilité de fonctionnalités cachées, afin de prévenir toute modification non autorisée des informations et d'instaurer la confiance quant à l'exactitude, l'exhaustivité et la fiabilité des informations.

**M. James M. Kilaba** (Directeur général de l'Autorité de régulation des communications de Tanzanie; TCRA) [[Biographie](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Kilaba)/[Présentation](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/GSSWTSA2016-Kilaba.pdf)] a mis en lumière les problèmes liés à la sécurité et à la protection de la vie privée découlant de l'évolution qu'ont connu les technologies, depuis l'époque où seuls quelques ordinateurs personnels étaient raccordés à l'Internet jusqu'à aujourd'hui, où n'importe qui ou n'importe quoi peut communiquer n'importe où et n'importe quand. M. Kilaba a décrit des initiatives mises en oeuvre aux niveaux national et régional pour protéger la vie privée, les données sécurisées et les infrastructures TIC, notamment la création d'une équipe nationale d'intervention en cas d'urgence informatique (TZ-CERT), chargée de diffuser auprès de diverses parties prenantes les connaissances, les informations et les compétences en matière de cybersécurité; la mise en oeuvre de la norme DNSSEC dans le système de registre des noms de domaine et l'organisation de discussions sur la cybersécurité au sein de l'Organisation des communications de l'Afrique de l'Est (EACO). M. Kilaba a appelé de ses voeux l'adoption d'une approche globale pour résoudre ces problèmes et souligné la nécessité d'harmoniser les normes internationales pour aider les pays en développement.

**M. Chawki Gaddes** (Président, Autorité nationale de protection des données personnelles, Tunisie) [[Biographie](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Gaddes)/[Présentation](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/GSSWTSA2016-Kilaba.pdf)] a décrit le rôle de premier plan que joue la Tunisie pour garantir, par sa Constitution, la protection de la vie privée et des données personnelles (Article 24, 2014), l'accès aux réseaux d'information et de communication (Article 32, 2004) et l'accès aux documents officiels (entrée en vigueur en 2017). Il a insisté sur le fait que la Tunisie accorde une grande d'importance à la création d'un espace de confiance entre la population, le secteur privé et les pouvoirs publics.

Session 3: Comment le secteur privé répond aux attentes des utilisateurs finals en matière de sécurité, de vie privée et de confiance

**M. Ilias Chantzos** (Directeur principal, Affaires gouvernementales, EMEA & APJ, Conseiller mondial pour la protection des infrastructures essentielles et de la vie privée, Symantec, Etats-Unis) a été le modérateur d'une session en deux parties sur la manière dont le secteur privé satisfait aux principes réglementaires en matière de sécurité, de vie privée et de confiance et répond aux attentes des utilisateurs finals à ce sujet.

**M. Ammar Alkassar** (P.-D. G., Rohde & Schwarz Cybersecurity, Allemagne) [[Biographie](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Alkassar)/[Présentation](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/3-1201601024_ITU%20GSS16_ALKASSAR_2.pptx)] a présenté les tendances dans le domaine des TIC qui transformeront notre monde durablement. Il a expliqué comment la cybersécurité serait un catalyseur indispensable de cette transformation et deviendrait encore plus essentielle dans l'avenir. M. Alkassar a souligné que les outils de sécurité déployés aujourd'hui sont loin d'être suffisants, vu les valeurs économiques à protéger. Il a indiqué qu'il est nécessaire de définir de nouveaux ensembles de normes car le paradigme en matière de sécurité des technologies de l'information a évolué afin de faire face à un environnement où les menaces sont de plus en plus intelligentes. Selon Rohde & Schwarz, ce nouveau paradigme comprendrait les éléments suivants: mettre en oeuvre la sécurité dès la conception et utiliser des mesures de prévention plutôt que de réaction; s'appuyer sur le contrôle des flux d'informations plutôt que sur le contrôle d'accès; et ne plus imposer aux utilisateurs des responsabilités qu'ils ne peuvent assumer en ce qui concerne la cybersécurité. M. Alkassar a fait remarquer que l'UIT et ses membres peuvent apporter des contributions importantes dans ce domaine, en particulier dans le cadre de leurs activités de normalisation, et dans l'instauration d'un lien entre la communauté des télécommunications traditionnelles et les nouveaux acteurs dans le secteur des TIC.

**M. Thomas Kremer** (Membre du directoire pour la confidentialité des données, les affaires juridiques et la conformité, Deutsche Telekom, Allemagne) [[Biographie](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Kremer)/[Présentation](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/Deutsche%20Telekom%20-%20final.pptx)/[Document de référence](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/Getting%20out%20of%20the%20digital%20trust%20trap%20-%20deutsche%20telekom.pdf)] a souligné que la transparence était une condition préalable à l'instauration de la confiance. Chacun doit pouvoir connaître l'utilisation qui est faite de ses données et décider en connaissance de cause d'accepter ou non une telle utilisation. Toutefois, le seul critère de la transparence est insuffisant si les entreprises veulent se montrer à la hauteur de leur responsabilité en matière de numérique. M. Kremer a appelé à la mise en place de systèmes capables de rendre les données anonymes, et ce de façon fiable, dans tous les cas d'utilisation, sans nécessiter l'action directe d'un utilisateur. Il considère que le cryptage est également un moyen de gagner la confiance de ses clients, notamment lorsque l'on a affaire à des données sensibles, liées à la santé, par exemple. Selon Deutsche Telekom, toute proposition visant à doter les autorités de "clés de réserve" ou de "portes dérobées" afin de sécuriser les systèmes se révèlerait contre-productive et minerait les efforts visant à améliorer la sécurité, puisque ces dispositifs seraient aussitôt exploités par des adversaires. M. Kremer a appelé à l'élaboration de solutions intelligentes, utilisables et applicables en temps utile dans le domaine de la cybersécurité. Alors que de nouvelles technologies voient le jour (Internet des objets, apprentissage automatique et informatique quantique, etc.), les attaques devraient être de plus en plus sophistiquées. Il est donc nécessaire d'adopter des approches normalisées afin d'identifier les risques et les attaques et de les atténuer.

**M. David Francis** (Responsable de la cybersécurité pour l'Europe, Huawei Technologies, Chine) [[Biographie](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Francis)/[Présentation](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/Huawei%20-%20final.pptx)] a exposé les tenants et les aboutissants de la protection de la vie privée et de la sécurité du point de vue des fournisseurs de technologies. Il a présenté les politiques et les procédures en vigueur dans une entreprise telle que Huawei Technologies afin de garantir la sécurité et la résilience de ses produits et qui, en définitive, contribuent à protéger la vie privée et les données de l'utilisateur final. Les principaux éléments à prendre en considération dans le cadre d'une approche globale sont les suivants: les dispositifs sécurisés; l'architecture (un réseau est construit à partir de multiples produits complexes); et les personnes, qui mettent en oeuvre, gèrent, modernisent, définissent et évaluent l'environnement.

M. Francis a évoqué la nécessité de gérer la chaîne d'approvisionnement mondiale dont dépend entièrement le secteur des TIC afin de limiter les risques pour la sécurité, mais aussi l'importance de la transparence et de la normalisation mondiale ainsi que la nécessité d'établir une coopération internationale pour améliorer la cybersécurité dans le monde.

**Mme Jaya Baloo** (Chef de la sécurité informatique, KPN, Pays-Bas) [[Biographie](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Baloo)/[Présentation](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/3-4ITU-GSS-Tunesia.pdf)] a parlé de la course aux technologies quantiques, de l'informatique à la cryptographie quantique. La disponibilité d'un ordinateur quantique représentera un risque pour la sécurité dans le cas des pays et des entreprises qui s'appuient sur la cryptographie asymétrique (systèmes RSA, ECC). Les mesures requises souhaitées sont des solutions post-quantiques, qui peuvent être mises en oeuvre en trois étapes. Tout d'abord, en allongeant les clés des algorithmes cryptographiques actuels. Deuxièmement, en utilisant la distribution de clés quantiques pour certains points critiques dans les réseaux. Troisièmement, en établissant et en prenant en charge des algorithmes cryptographiques post-quantiques pérennes. Les spécialistes mondiaux de la sécurité de l'information accomplissent actuellement des progrès considérables en matière d'innovation dans le domaine des technologies quantiques. Toutefois, le risque est qu'une nouvelle fracture numérique se créé en matière de sécurité, entre les pays qui ont les ressources financières et universitaires nécessaires pour posséder un ordinateur quantique leur permettant de percer la cryptographie des autres pays tout en protégeant leurs propres communications et les pays qui ne peuvent ni attaquer ni se défendre.

**M. James Snow** (Responsable des stratégies en matière de sécurité et de conformité, Google, Etats‑Unis) [[Biographie](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Snow)/[Présentation](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/Google-final.pptx)/[Document de référence](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/GoogleExecSummary_2016.pdf)] a déclaré que l'une des priorités de Google était de gagner et de conserver la confiance des consommateurs en traitant les données dans un environnement sûr, fiable et conforme. La sécurité et la vie privée revêtent une importance centrale pour Google, qui investit beaucoup dans la protection des données de ses clients, notamment par l'utilisation de serveurs et d'infrastructures de réseau spécialisés et sécurisés, et par le cryptage des données des clients, que celles-ci soient stockées sur un disque ou dans des supports de sauvegarde ou qu'elles circulent sur l'Internet ou entre les centres de traitement des données.

M. Snow a fait savoir qu'il n'y a pas de confiance du consommateur sans compréhension, et que la compréhension ne peut se fonder que sur la transparence, c'est-à-dire sur la mise à disposition d'une documentation approfondie, de rapports d'audits et de certifications. Google reconnaît que la coopération internationale joue un rôle important et exploite plusieurs normes internationales sur la sécurité et la vie privée, notamment:

• la norme ISO 27001:2013, Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Exigences;

• la norme ISO 27017:2015, Technologies de l'information – Techniques de sécurité – Code de pratique pour les contrôles de sécurité de l'information fondés sur l'ISO/IEC 27002 pour les services du nuage;

• la norme ISO 27018:2014, Technologies de l'information – Techniques de sécurité – Code de bonnes pratiques pour la protection des informations personnelles identifiables (PII) dans l'informatique en nuage public agissant comme processeur de PII; et

• les rapports SOC 2 et SOC 3, qui fournissent un cadre de vérification fondé sur des principes non liés à la vie privée, à savoir la sécurité, l'accessibilité, l'intégrité du traitement et la confidentialité.

**M. Yuejin Du** (Vice-Président pour la sécurité, Alibaba Group, Chine) [[Biographie](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Du)/[Présentation](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/Yuejin-DU.pptx)] a donné des détails sur l'importance de la sécurité et de la vie privée dans les infrastructures que le Groupe fournit à ses clients dans le domaine du commerce et des technologies liées aux données. Alibaba fournit par exemple des produits relatifs à la sécurité des informations à ses partenaires et encourage la normalisation dans le cadre de l'Alliance de sécurité pour l'écosystème de commerce électronique (EESA), qu'il a lancée en juillet 2016. Dans le cadre de l'EESA, Alibaba et ses partenaires peuvent mettre à profit les modèles de détection des risques établis pour étudier et identifier les menaces, et travailler de concert afin de renforcer la sécurité et de protéger la vie privée dans l'écosystème de commerce électronique en appliquant les normes définies par l'Alliance.

**M. Bernard** **Benoit** (Directeur général, WhiteNoise/Kudelski Security, Suisse) [[Biographie](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Benoit)/[Présentation](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/Kudelski%20-%20final.pdf)] a évoqué les conflits d'intérêts éventuels entre les utilisateurs, les fournisseurs de services et les gouvernements, et a fait observer que les réseaux de télécommunication présentaient de nombreuses failles de sécurité et qu'ils étaient, de fait, incapables de garantir la sécurité et la confidentialité des communications. Pour renforcer la sécurité et la protection de la vie privée dans des réseaux non fiables, il a recommandé d'adopter une approche des services OTT (over-the-top) fondée sur un composant matériel de sécurité modulable fonctionnant indépendamment des réseaux et des protocoles sous-jacents. M. Benoit a rappelé aux participants qu'il était nécessaire de mettre en oeuvre des solutions qui soient indépendantes vis‑à‑vis des plates-formes et dotées d'interfaces normalisées conformes aux dispositions légales applicables en matière d'interception, sans mettre en péril l'intégrité des technologies par l'utilisation de portes dérobées, de clefs de réserve, etc.

Session 4: Approche des organismes de normalisation concernant la sécurité, la vie privée et la confiance

La session 4 a consisté en un examen des approches adoptées par divers organisations de normalisation concernant la sécurité, la vie privée et la confiance. Le modérateur de la session était **M. Toni Eid** (Editeur en chef, Telecom Review) [[Biographie](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Eid)].

**Mme Sophie Clivio** (Directrice chargée de la normalisation et des politiques techniques, Organisation internationale de normalisation (ISO)) [[Biographie](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Clivio)/[Présentation](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/ISO%20-%20final.PPTX)] a présenté l'approche globale et multi-sectorielle adoptée par l'ISO quant à la sécurité, la vie privée et la confiance. Elle a mis en évidence les travaux des comités de l'ISO sur la sécurité et la résilience, la gestion des risques, la chaîne de blocs et les technologies de registres numériques distribués, et les activités conjointes ISO/CEI sur la sécurité et la confidentialité des informations menées par le Comité technique mixte pour les technologies de l'information (JTC 1). Les domaines d'études principaux du JTC 1 sont les suivants: gestion de la sécurité de l'information, cryptographie et gestion de la sécurité, gestion d'identité et technologies de protection de la vie privée, biométrie, identification des cartes et des personnes, gouvernance des technologies de l'information, mécanismes liés à la sécurité, à la vie privée et à la confiance dans l'informatique en nuage, mégadonnées et Internet des objets. Mme Clivio a fait observer que l'ISO et ses normes jouent un rôle dans de nombreux secteurs économiques, notamment la santé, les transports (par exemple dans l'aviation, les systèmes de transport intelligents, les technologies marines), l'énergie, le bâtiment et l'industrie (notamment la fabrication additive). Elle a également indiqué que des accords de coopération avaient été conclus avec des organisations pour répondre aux besoins et aux spécificités de ces secteurs.

**M. Frans Vreeswijk** (Secrétaire général et P.-D. G., Commission électrotechnique internationale (CEI)) [[Biographie](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Vreeswijk)/[Présentation](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/IEC%20-%20final.pptx)] a expliqué le cadre que la CEI offre à toutes les parties prenantes dans le domaine de l'électrotechnique, afin d'instaurer la confiance dans des produits et des systèmes sûrs et efficaces moyennant l'utilisation des normes internationales et des systèmes d'évaluation de la conformité de la CEI. La CEI a publié plus de 200 normes relatives à la cybersécurité, traitant en particulier de la protection des infrastructures essentielles, comme les infrastructures de production et de distribution d'électricité, les infrastructures de gestion de l'eau et des déchets, les hôpitaux et les établissements de soins de santé, les centres industriels et les centres de données, contre les cybervulnérabilités et les cyberattaques. La CEI apporte en outre une contribution essentielle à la sûreté et à la sécurité de tous les équipements électriques et électroniques permettant la collecte ou l'accès aux données et la prise en charge des protocoles de commande. Parmi ces équipements, on trouve par exemple des capteurs, des dispositifs médicaux, des dispositifs intelligents portables ainsi que des technologies de calcul et de stockage des données. Les normes internationales de la CEI sont indispensables pour améliorer la résilience, la gestion des risques et l'efficacité.

La CEI travaille en étroite collaboration avec l'ISO dans le cadre du Comité technique mixte sur les technologies de l'information (ISO/CEI JTC 1) dans des domaines comme la gestion de la sécurité de l'information, la gestion d'identité, la cryptographie et l'identification de sécurité, les technologies de protection de la vie privée, la biométrique, les cartes et les systèmes d'identification personnelles, l'informatique en nuage, les mégadonnées, et bien d'autres domaines encore. La CEI entretient un dialogue constant avec l'UIT, ainsi qu'avec l'ISO dans le cadre de la Coopération en matière de normalisation mondiale.

M. Vreeswijk a appelé à une coopération plus étendue entre toutes les organisations de normalisation dans les domaines de la sécurité, de la vie privée et de la confiance. En substance, aucune organisation ne sera en mesure de fournir à elle seule toutes les normes nécessaires dans ces domaines.

**Mme Karen McCabe** (Directrice principale, Politique en matière de technologie et affaires internationales, Institute of Electrical and Electronics Engineer Standards Association (IEEE-SA)) [[Biographie](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#McCabe)/[Présentation](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/IEEE-final.pptx)] a souligné le rôle crucial des normes pour garantir la sécurité, protéger la vie privée, et instaurer la confiance dans les TIC. Pour que les normes puissent remplir ce rôle, la meilleure méthode consiste à suivre un ensemble de principes garantissant à l'échelle mondiale une coopération volontaire entre les parties intéressées et les parties prenantes, et favorisant l'excellence, l'interopérabilité mondiale et l'innovation sur le plan technique. Il s'agit notamment des principes suivants: participation directe, procédure appliquée dans les règles, large consensus, équilibre, transparence, libre accès universel, cohérence et dimension développement.

Mme McCabe a noté que, dans l'optique de la sécurité, les processus ouverts sont efficaces, car l'examen par plusieurs spécialistes peut révéler d'éventuelles failles et améliorer les normes qui sont en cours d'élaboration. Des normes ouvertes élaborées en toute transparence contribuent à une plus grande confiance dans les plates-formes, les services et les produits qui sont fondés sur ce type de normes et les respectent. En outre, les normes ouvertes contribuent à l'utilisation généralisée des technologies respectueuses de la vie privée et de la sécurité, dans la mesure où celles-ci favorisent l'interopérabilité. En conclusion, Mme McCabe a fait valoir que les normes ouvertes stimulent l'innovation, ce qui peut esquisser des solutions pour résoudre les problèmes liés à la sécurité, à la vie privée et à la confiance.

L'IEEE dispose d'un grand nombre de normes qui touchent à la sécurité, à la vie privée et à la confiance, notamment la série IEEE 802 des normes sur les réseaux, la série IEEE 1363 sur la cryptographie (axée sur les algorithmes à infrastructure de clés publiques (PKI)), la série IEEE 1619, et de nombreuses autres séries. Le Groupe ICSG (Industry Connections Security Group) de l'IEEE se compose d'entités s'occupant de sécurité informatique qui se sont regroupées pour mettre en commun leur expérience et leurs ressources pour lutter contre l'augmentation systématique et rapide des menaces pour la sécurité informatique. Une autre initiative récente, l'initiative de l'IEEE sur l'Internet, visait à accroître l'influence et la réputation de l'IEEE en ce qui concerne l'élaboration de politiques mondiales, dans les domaines de la gouvernance de l'Internet, de la cybersécurité et de la confidentialité des données, en fournissant un ensemble consensuel de connaissances techniques et scientifiques approfondies, ainsi que des orientations en la matière. Les responsables de l'initiative mondiale de l'IEEE relative à la prise en compte des questions éthiques dans la conception de systèmes autonomes et le Comité ad hoc sur l'éthique, la société et la technologie réfléchissent à de nouvelles normes et solutions, ainsi qu'à de nouvelles certifications et de nouveaux codes de conduite, et cherchent à faire naître un consensus pour une utilisation éthique des technologies intelligentes, y compris l'intelligence artificielle et les systèmes autonomes.

Mme McCabe a préconisé qu'une nouvelle génération de professionnels spécialistes des questions de confidentialité des données, de sécurité et d'éthique et venant d'horizons divers soit associée au processus d'élaboration de normes et également que les questions de confidentialité des données, de sécurité et d'éthique soient prises en compte dans les normes ouvertes, afin de contribuer à renforcer la confiance dans les TIC.

**M. Ashok Ganesh** (Responsable de l'innovation, CEN-CENELEC) [[Biographie](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Ganesh)/[Présentation](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/CEN-CENELEC-final.pptx)] a souligné que tous les secteurs industriels connaissent des bouleversements, du fait de l'utilisation des technologies et des méthodes numériques (par exemple l'Internet des objets, l'informatique en nuage, la robotique et les technologies de capteurs), qui transforment radicalement les processus et les systèmes de ces secteurs, et même leurs modèles d'activité économique. Ces secteurs industriels traditionnels verticaux (par exemple industrie de transformation, énergie et transport), qui, dans le passé, n'utilisaient que très peu les TIC et les technologies numériques, recherchent une aide et des solutions normatives pour pouvoir opérer cette transformation. M. Ganesh a observé que des organisations de normalisation telles que l'ISO, la CEI, ainsi que le Comité européen de normalisation (CEN) et le Comité européen de normalisation électronique (CENELEC), ont une "empreinte" importante dans ces secteurs verticaux et souhaitent développer leurs méthodes pour répondre aux besoins dans le domaine des TIC et des technologies numériques. L'adoption de ces technologies suppose l'utilisation de systèmes de production industrielle et de procédés de fabrication et entraînera la génération, le traitement, le partage et le stockage d'énormes volumes de données. M. Ganesh a souligné que le défi pour les organisations de normalisation est multiple à savoir: conserver la coopération des parties prenantes traditionnelles; attirer des parties prenantes du secteur des TIC/du secteur du numérique; et repenser leurs propres stratégies afin d'être en mesure de proposer directement et indirectement des solutions en matière de normalisation dans un environnement de plus en plus complexe et en évolution rapide. L'une des priorités pour les organisations de normalisation est de mettre l'accent sur les besoins et les applications des secteurs verticaux, et d'examiner le lien entre la cybersécurité et la sécurité fonctionnelle, la fiabilité du produit, ainsi que la sécurité et la confidentialité des données.

**M. Reinhard Scholl** (Adjoint au Directeur, Bureau de la normalisation des télécommunications de l'UIT) [[Biographie](http://www.itu.int/en/ITU-T/wtsa16/gss/Pages/bios.aspx#Scholl)/[Présentation](http://www.itu.int/en/ITU-T/wtsa16/gss/Documents/Presentations/Reinhard-final.pptx)] a rappelé à tous les participants qu'un colloque sur la cybersécurité avait eu lieu en marge de l'AMNT-04 à Florianopolis (Brésil). Les conclusions de cette manifestation étaient composées de onze messages principaux, dont la plupart sont toujours valides aujourd'hui, par exemple "La sécurité doit être intégrée et non pas rajoutée", "Les diverses parties prenantes doivent partager les informations dont elle dispose" et "La normalisation est nécessairement une composante vitale de l'approche mondiale de la cybersécurité".

Pour illustrer la situation actuelle, M. Scholl a donné certains chiffres relatifs au nombre de cyberincidents connus ayant visé l'infrastructure de réseau de l'UIT. Il a indiqué que, selon lui, sécurité et protection de la vie privée ne s'excluent pas mutuellement. Il a en outre expliqué que l'UIT n'avait cessé d'intensifier ses travaux pour renforcer la confiance et la sécurité dans l'utilisation des TIC afin de faciliter la mise en place d'infrastructures de réseau, de services et d'applications plus fiables. M. Scholl a présenté les travaux récents de l'UIT relatifs à la sécurité et à la confiance, notamment un rapport qui souligne l'importance et la nécessité de la confiance dans le contexte des TIC, et qui définit les principales caractéristiques de la confiance, ainsi que des notions connexes. L'une des idées présentées dans ce rapport concerne un "indice de confiance", regroupant de multiples indicateurs relatifs à la confiance en une seule mesure de référence exprimée sous la forme d'un nombre. On pourrait utiliser un indice pour comparer la confiance entre des parties prenantes qui établissent une nouvelle relation de confiance ou une chaîne de valeur de confiance.

M. Scholl a noté que les membres de l'UIT ont entrepris des travaux dans de nombreux domaines, exigences, capacités et scénarios de services liés à l'instauration de la confiance; cadre architectural pour des réseaux de télécommunication fiables, solutions techniques pour l'instauration de la confiance; instauration de la confiance et analyse des mégadonnées; et la gestion de la confiance pour les échanges inter-nuages entre autres. L'UIT a engagé des travaux de normalisation connexes, dans les domaines suivants: cybersécurité, gestion de la sécurité, architectures et cadres de sécurité, lutte contre le spam, gestion d'identité et protection des informations d'identification personnelle.

En outre, M. Scholl a recommandé d'étudier la contribution que la communauté des logiciels à code source ouvert peut apporter pour ce qui est des normes de sécurité, de protection de la vie privée et de confiance dans l'infrastructure et les services TIC. Il a indiqué que de nouvelles activités devraient être menées afin de faciliter la collaboration entre les communautés open source et les spécialistes de la normalisation, ce qui permettrait de garantir un haut niveau de qualité pour les normes et les implémentations logicielles.

# Notes

1. Voir par exemple la Recommandation UIT-T X.1171: "Menaces et protection requise pour les informations d'identification personnelle dans les applications utilisant l'identification par étiquette". [↑](#endnote-ref-1)
2. Voir par exemple la Résolution 130 (Rév. Busan 2014) de la Conférence de plénipotentiaires, sur le renforcement du rôle de l'UIT dans l'instauration de la confiance et de la sécurité dans l'utilisation des technologies de l'information et de la communication. [↑](#endnote-ref-2)
3. <http://www.un.org/fr/universal-declaration-human-rights/> [↑](#endnote-ref-3)
4. <http://www.ohchr.org/fr/professionalinterest/pages/ccpr.aspx> [↑](#endnote-ref-4)
5. <http://www.un.org/documents/ga/res/45/a45r095.htm>; UN Doc E/CN.4/1990/72 <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G90/107/08/PDF/G9010708.pdf?OpenElement> [↑](#endnote-ref-5)
6. <https://www.coe.int/fr/web/conventions/full-list/-/conventions/rms/0900001680078b37> [↑](#endnote-ref-6)
7. <http://www.echr.coe.int/Documents/Convention_FRA.pdf> [↑](#endnote-ref-7)
8. <https://www.oas.org/dil/treaties_B-32_American_Convention_on_Human_Rights.htm> [↑](#endnote-ref-8)
9. Voir par exemple le Cadre de protection des renseignements personnels de l'APEC et le Cadre réglementaire de l'UE relatif à la vie privée. Ces textes se sont inspirés, dans une certaine mesure, des Lignes directrices de l'OCDE régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel, <http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf>. [↑](#endnote-ref-9)
10. Déclaration de Montreux sur la Conférence internationale des Commissaires à la protection des données et de la vie privée, <https://icdppc.org/wp-content/uploads/2015/02/Montreal-Declaration-French.pdf>. [↑](#endnote-ref-10)
11. Résolution 68/167 de l'Assemblée générale des Nations Unies, <http://www.un.org/fr/ga/search/view_doc.asp?symbol=A/RES/68/167>.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_ [↑](#endnote-ref-11)