Nations Unies ECE/TRADE/C/CEFACT/2022/13

Conseil économique et social

Distr. générale
19 juillet 2022
Français
Original : anglais

Commission économique pour l'Europe

Comité exécutif

Centre pour la facilitation du commerce et les transactions électroniques

Vingt-huitième session
Genève, 10 et 11 (matin) octobre 2022
Point 5 d) de l'ordre du jour provisoire
Recommandations et normes :
Documents d'aide à l'application

Rapport du Domaine gestion des données électroniques (eDATA) sur les normes de l'Internet des objets pour la facilitation du commerce

Établi par le Bureau

Résumé

L'Internet des objets (IoT) facilite le commerce en permettant la collecte et l'échange transfrontalier d'informations électroniques sans intervention humaine, ce qui le rend plus sûr, plus efficace et plus économique. Dans le présent rapport, on fait ressortir le rôle que, compte tenu de l'utilisation généralisée de l'intelligence des objets, les normes du Centre des Nations Unies pour la facilitation du commerce et les transactions électroniques (CEFACT-ONU) peuvent jouer dans la définition des flux de données et de processus entre les objets connectés exploités par diverses parties dans le cadre d'une chaîne d'approvisionnement internationale et évoque les modalités de l'intégration interopérable de ces données dans les processus existants d'automatisation de la chaîne d'approvisionnement. Le rapport donne des exemples de normes d'échange de données, de processus et d'informations sur l'IoT, et recense les besoins de données pour une adoption plus large de l'IoT dans les applications de facilitation du commerce.

Publié sous la cote ECE/TRADE/C/CEFACT/2022/13, le présent document est soumis par le secrétariat à la vingt-huitième session pour qu'il en soit pris note.

I. Introduction

1. L'Internet des objets (IoT) est un réseau qui relie à l'Internet des « objets » dont l'identification est unique. Ces appareils connectés ont des capacités de détection et peuvent être programmés. L'exploitation de leur identification unique et de leurs capacités de détection permet de recueillir des informations sur ces appareils et d'en modifier l'état.

2. Les principales caractéristiques d'un écosystème d'objets ou d'appareils connectés (aussi appelé écosystème IoT) sont les suivantes :

- Interconnexions avec et entre les appareils ;
- Identification unique des appareils ;
- Capacités sensorielles ;
- Intelligence embarquée ;
- Capacités de communication ;
- Programmabilité.

3. Ces écosystèmes IoT rendent possibles des applications inédites qui facilitent le commerce transfrontalier sans papier grâce à l'utilisation d'appareils connectés qui détectent, collectent, traitent, partagent et exploitent les données. Des données telles que la température, l'humidité et la localisation peuvent être recueillies à partir d'appareils connectés et être utilisées pour alimenter un certain nombre d'applications allant de la capacité de garantir la fraîcheur des produits tout au long d'une chaîne d'approvisionnement, au suivi de la localisation des actifs, en passant par la détection de défaillances du matériel dans la logistique et le transport.

4. Les appareils connectés ont également la capacité de recueillir et d'enregistrer des données en temps réel et de manière continue, et de les associer à des identifiants uniques. Ils peuvent donc servir à retracer l'origine des données à partir de relevés de capteurs de base, même si ces données sont exploitées par des applications logicielles pour créer des informations dérivées complexes. On peut introduire ces données en temps réel dans des systèmes de décision d'une chaîne d'approvisionnement internationale, notamment pour pousser davantage l'automatisation ou prendre d'autres décisions, comme le montre le projet sur les conteneurs intelligents du Centre des Nations Unies pour la facilitation du commerce et les transactions électroniques (CEFACT-ONU).

5. L'IoT offre des possibilités intéressantes pour la facilitation du commerce car il permet de créer et d'échanger des informations électroniques transfrontalières sans intervention humaine, donc de manière plus sûre, plus efficace et plus économique. Les systèmes IoT peuvent également servir à garantir l'intégrité des données sur l'état physique des objets, le conditionnement, les véhicules et les conteneurs.

6. En combinaison avec d'autres technologies nouvelles telles que les chaînes de blocs, les réseaux 5G, les interfaces de programmation d'applications (API) et les plateformes en nuage, l'IoT pourrait avoir un impact énorme sur la volonté d'automatiser considérablement les chaînes d'approvisionnement internationales et de faciliter le commerce sans papier transfrontalier.

7. Il existe déjà de nombreux projets dans le monde qui s'emploient à révolutionner les chaînes d'approvisionnement en utilisant les gains d'efficacité produits par l'IoT pour un meilleur suivi des actifs, la gestion des stocks et la maintenance préventive du matériel. Le projet sur les conteneurs intelligents du CEFACT-ONU en est un exemple intéressant. On y étudie comment les conteneurs intelligents (conteneurs maritimes normalisés équipés de capteurs) permettent le suivi et la surveillance de porte à porte. Ces conteneurs peuvent favoriser la visibilité et la transparence de bout en bout tout au long de la chaîne d'approvisionnement.

8. Compte tenu de l'utilisation généralisée de l'IoT dans un large éventail de systèmes et de son potentiel s'agissant d'améliorer les canaux de communication existants et d'en créer de nouveaux, le présent document vise à mettre en évidence l'utilité des normes et le rôle que

le CEFACT-ONU peut jouer dans l'élaboration ou l'élargissement des exigences techniques existantes, l'objectif étant de porter à son maximum la valeur de cette technologie pour les membres du CEFACT-ONU.

9. Le présent rapport porte sur le rôle que les normes du CEFACT-ONU peuvent jouer dans la définition des flux de données et de processus entre les appareils connectés exploités par diverses parties dans le cadre d'une chaîne d'approvisionnement internationale et sur les modalités de l'intégration interopérable de ces données dans les processus existants d'automatisation des chaînes d'approvisionnement.

II. Normes relatives aux données

10. L'IoT peut donner un sens à ce qui se passe dans le monde physique en recueillant des données qui proviennent des mouvements physiques et des changements intervenant au niveau de l'environnement. Au début du processus, il y a les capteurs, qui enregistrent les mouvements physiques des personnes, des animaux, des automobiles ou encore des colis, ou les changements dans l'environnement tels que la température ou l'humidité. Ces données brutes sont ensuite transmises à un dispositif de passerelle qui les convertit en un format de données transmissible conforme au protocole Internet (IP) et les envoie à des serveurs, sur place ou dans le nuage, à des fins de stockage et de calcul. Ensuite, les données sont de nouveau reformulées dans un format normalisé afin que leur contenu puisse être compris et utilisé pour obtenir les meilleurs résultats possibles.

11. Le projet sur les conteneurs intelligents du CEFACT-ONU est un exemple de projet IoT qui a exploité la bibliothèque de composants communs (CCL) du CEFACT-ONU. Ce projet occupe une place importante dans l'élaboration de normes multimodales internationales qui appuieront l'avenir du commerce mondial. Le conteneur intelligent est un conteneur d'expédition maritime équipé d'un dispositif de surveillance intelligent installé de façon permanente. Ce dispositif comporte un ensemble de capteurs intégrés au conteneur, ce qui lui permet de relever en temps réel des informations telles que la localisation, l'ouverture et la fermeture des portes, les vibrations, la température, l'humidité et d'autres paramètres physiques mesurables de l'environnement dans lequel se trouvent les marchandises à l'intérieur du conteneur, ainsi que du conteneur lui-même. Il dispose également de capacités de communication (utilisées pour envoyer les données mesurées à un centre de collecte) et peut être associé à des capteurs distants supplémentaires pour répondre aux besoins spécifiques d'une cargaison donnée.

12. Dans le cadre du processus de modélisation des données, le projet Smart Container a ajouté de nouveaux éléments à la CCL et au modèle de données de référence pour le transport multimodal afin de saisir les éléments suivants :

- Éléments et classes de données liés aux capteurs ;
- Éléments et classes de données d'information géographique ;
- Les entités de liaison du modèle de données de référence pour le transport multimodal, comme les expéditions et le matériel de transport.

13. Les conteneurs intelligents présentent certes un exemple intéressant de l'utilisation des normes du CEFACT-ONU dans l'IoT ; cela dit, à mesure que l'utilisation de l'IoT se développe dans le transport et le commerce, le modèle de données de la CCL peut être amélioré et contribuer à mieux répondre à l'évolution des exigences commerciales suscitées par le nombre croissant d'applications IoT.

III. Normes relatives aux processus

14. Diverses technologies peuvent rendre les chaînes d'approvisionnement plus efficaces grâce à un échange opportun des informations tout au long des différentes étapes de ces chaînes. L'IoT fait partie des technologies qui fluidifient les échanges de données grâce à l'utilisation de nombreux capteurs qui fournissent des informations telles que les conditions atmosphériques, la température, les chocs et les vibrations, la position GPS, etc. Une fois

obtenues via un dispositif IoT, ces données peuvent être utilisées comme entrées pour des programmes qui modifient à distance les paramètres, contrôlent l'environnement et fournissent l'atmosphère voulue pour maintenir la qualité des marchandises. Elles peuvent également être utilisées pour d'autres processus tels que les déclarations de dommages.

15. Il existe de multiples possibilités d'améliorer l'efficacité du commerce transfrontalier sans papier par les normes relatives aux processus du CEFACT-ONU conformes à l'IoT. L'un des principaux obstacles à l'adoption harmonieuse des systèmes IoT réside dans la réticence des autorités à céder le contrôle de leurs données et de leurs processus à des plateformes partagées qui échappent à leur compétence[1]. Pour surmonter cette réticence, il convient d'établir des processus qui permettront de partager de manière appropriée les données enregistrées au-delà des frontières et sur différentes plateformes sans violer les normes de confidentialité et de réglementation.

16. Le projet sur les conteneurs intelligents est un excellent exemple de la façon dont l'IoT peut être exploité dans la chaîne d'approvisionnement. Le CEFACT-ONU a fixé des spécifications relatives aux exigences opérationnelles (BRS) pour les conteneurs intelligents qui sont les premières normes officielles détaillant les éléments de données utilisés dans les applications desdits conteneurs. Il est important d'adhérer à ces normes, car le passage généralisé à des conteneurs intelligents est bien nécessaire pour les différentes parties prenantes, les systèmes IoT basés sur des normes pouvant favoriser davantage cette évolution. La normalisation des conteneurs intelligents a tout son sens parce qu'elle permettra de réduire les coûts de déploiement et de développement des solutions IoT[2], nécessaires pour réduire les délais d'expédition et les risques pour toutes les parties

17. Les normes des processus commerciaux du modèle acheter-expédier-payer du CEFACT-ONU[3] ont servi de référence pour l'application des BRS du CEFACT-ONU[4]. Ce modèle décrit les principales parties impliquées dans la chaîne d'approvisionnement internationale ainsi que les opérations successives qui la composent, et établit une relation entre les entités de données utilisées dans les différentes parties de la chaîne d'approvisionnement, allant des contrats de transport aux contrats de vente internationaux. Ces modalités de fonctionnement sont interdépendantes dans le cadre du modèle « acheter-expédier-payer », qui comprend le transport et la logistique opérationnels, les contrats de transport, le dédouanement et les procédures réglementaires et financières, et qui permet d'échanger des informations tant à l'intérieur des zones commerciales qu'entre celles-ci.

18. Le modèle « acheter-expédier-payer » peut être appliqué par n'importe quelle région, n'importe quel secteur d'activité ou n'importe quel pays pour créer des documents d'échange de données électroniques relatifs au transport et au commerce, qui sont ensuite intégrés dans des solutions logicielles destinées aux transporteurs, aux agents, aux négociants, aux douanes, aux transitaires, etc. Le modèle est également utile pour appuyer et développer la mise en œuvre de guichets uniques, car il fournit la base de l'harmonisation des données et des spécifications d'échange de données harmonisées au niveau mondial dans la chaîne d'approvisionnement internationale. Les systèmes IoT peuvent encore améliorer les capacités du modèle acheter-expédier-payer en exploitant les normes existantes et établies pour les processus d'achat-expédition-paiement et en les développant davantage pour les rendre compatibles avec les informations reçues par les systèmes IoT.

19. Les données générées par les dispositifs reliés à l'IoT appartiennent généralement aux opérateurs des infrastructures, aux fournisseurs de services à valeur ajoutée ou à certaines plateformes, et l'accès à ces données passe par les interfaces de programmation d'application (API) des plateformes ou par l'utilisation de méthodes fondées sur l'échange de messages. L'établissement de normes dans le cadre des normes de processus métier « acheter-expédier-

[1] CEFACT-ONU, « White Paper: Technical Applications of Blockchain to UN/CEFACT Deliverables, version 2 », (2019) disponible sur https://www.unece.org/fileadmin/DAM/cefact/GuidanceMaterials/WhitePaperBlockchain_TechApplication.pdf.

[2] CEFACT-ONU, « Business Requirements Specification (BRS), Smart Containers », (2019).

[3] https://tfig.unece.org/contents/buy-ship-pay-model.htm.

[4] CEFACT-ONU, « Buy-Ship-Pay Reference Data Model, Version 1 », (2019). Disponible sur https://www.unece.org/fileadmin/DAM/cefact/brs/BuyShipPay_BRS_v1.0.pdf.

payer » pour gérer les données recueillies par l'IoT favorisera une croissance considérable du commerce international en raison de l'amélioration de la rapidité, de la qualité et des volumes des données de la chaîne d'approvisionnement, et contribuera aussi à favoriser l'adoption du modèle « acheter-expédier-payer ».

20. L'accent devrait être mis sur les plateformes partagées, car celles-ci permettront de mieux répartir les avantages des innovations grâce à l'échange des informations et à l'accès aux données sur demande. Les documents BRS ou les mappages des spécifications relatives aux exigences (RSM) doivent être structurés de manière à permettre l'échange d'informations au moyen de sites Web compatibles avec les plateformes qui offrent un accès privé/public à l'aide de protocoles tels que HTTP et permettent aux interfaces externes de programmation d'application d'ajouter des fonctionnalités et un accès aux données[5]. Les informations obtenues grâce aux dispositifs IoT pourront ainsi être utilisées à des fins d'efficacité, de réduction du recours aux intermédiaires et de diminution des coûts.

21. L'établissement de modèles sémantiques normalisés du CEFACT-ONU et l'adhésion à ces modèles pourraient susciter une extension des réseaux entre opérateurs économiques et favoriser l'intégration sur diverses plateformes. Le développement de BRS et de RSM connexes contribuera au déploiement de l'IoT à plus grande échelle. Tout comme elles ont été mises en conformité avec la norme EDIFACT-ONU[6] et le langage XML, les normes sémantiques du CEFACT-ONU devraient idéalement être mises en correspondance avec des technologies telles que l'IoT, la chaîne de blocs et les interfaces de programmation d'application des plateformes Web. Pour gérer les flux de données à un niveau plus granulaire, la modélisation de la sémantique détaillée des processus sera de plus en plus nécessaire.

22. L'intégration plus large de l'IoT avec d'autres technologies telles que la chaîne de blocs et l'intelligence artificielle pourrait susciter des occasions intéressantes de faciliter le commerce transfrontalier sans papier. À cette fin, les recommandations suivantes pourraient être envisagées pour améliorer les normes relatives aux processus[7] :

- Élaborer une architecture de référence pour promouvoir une compréhension complète des spécifications et des nouvelles technologies ;
- Revoir les modèles de processus existants pour les BRS/RSM pour permettre l'interopérabilité des données sur la chaîne de blocs (une fois que les données de l'IoT ont été enregistrées) afin de prendre en charge l'accès donné aux autorités des différents pays, en utilisant des contrats intelligents pour des événements allant de la libération des envois à l'approbation des factures ;
- Élaborer des modèles de processus plus granulaires axés sur l'état des cycles de vie des principales ressources le long des chaînes de valeur mondiales. Ces ressources vont des contrats et des paiements aux envois et aux conteneurs.

23. Les normes doivent être conçues de manière à créer une cohérence, de sorte que, quelle que soit la plateforme hébergeant les informations sur une ressource, tant que les normes sont appliquées, les parties prenantes peuvent interpréter les données de la même façon.

24. Les capacités des systèmes IoT sont encore améliorées lorsqu'on les associe à la technologie de la chaîne de blocs et à des données normalisées.

25. Les données normalisées recueillies à l'aide de capteurs IoT peuvent être stockées dans des registres numériques tiers (basés sur la technologie de la chaîne de blocs) et être utilisées pour la traçabilité des produits dans les chaînes d'approvisionnement. Cela permet de créer des données fiables aux applications multiples, notamment pour fournir la preuve du

[5] CEFACT-ONU, « White Paper: Technical Applications of Blockchain to UN/CEFACT Deliverables, v.2 », (2019).

[6] Règles des Nations Unies concernant l'échange de données informatisé pour l'administration, le commerce et le transport.

[7] CEFACT-ONU, « White Paper: Technical Applications of Blockchain to UN/CEFACT Deliverables, v.2 », (2019).

pays d'origine et des quantités expédiées, pour établir les déclarations de dommages dus à de mauvaises conditions de transport, etc.

26. Les registres (grands livres) numériques étant utilisés dans les processus commerciaux auxquels participent différentes parties, les applications devront prendre en charge les échanges de données entre différents registres numériques et il faudra donc fixer des normes pour faciliter les processus. Par exemple, à l'avenir, dans une transaction unique d'importation de bout en bout, il peut y avoir des échanges sur autant de registres numériques différents qu'il y a de participants au processus : l'importateur peut utiliser un registre électronique du financement de la transaction et l'exportateur, un autre, chacun ayant ses propres banques et, ensuite, chaque banque peut se servir de registres différents pour vérifier les licences et les certifications d'assurance qualité des produits. Ensuite, les compagnies d'assurance pourraient utiliser différents registres numériques pour la vérification et l'échange de données, tandis que les transporteurs/expéditeurs pourraient se servir du leur pour gérer les documents d'expédition. Enfin, il se peut que les douanes tiennent un autre registre pour vérifier les documents et contrôler le bon comportement de l'exportateur et de l'importateur par le passé.

27. Si les normes du CEFACT-ONU sont établies compte tenu des conditions créées par l'utilisation de dispositifs IoT et de registres numériques, l'échange de données ou l'interopérabilité entre plusieurs registres deviendra possible. Les capacités de l'IoT seront alors également renforcées, offrant plus de sécurité et de confidentialité dans la gestion des données. En un mot, les normes du CEFACT-ONU relatives aux processus peuvent être utiles pour soutenir l'adoption plus large de l'IoT parce qu'elles fixent des normes qui offrent une interopérabilité sémantique entre plusieurs registres.

IV. Normes relatives aux messages (échange d'informations)

28. Le présent document est centré sur la nécessité d'élaborer davantage le document BRS afin de prendre en charge les normes relatives aux messages internationaux pour échanger efficacement des informations sur l'IoT et les registres numériques. Certaines des caractéristiques les plus particulières de ces données sont la nécessité d'échanger des quantités relativement faibles de données (extraits) et/ou de grandes quantités de ces mêmes extraits de données. Par exemple, il est nécessaire de créer des structures de données et de messages cohérentes pouvant être utilisées pour échanger ce type de données entre différents modèles commerciaux tels que ceux des conteneurs intelligents, des portails de présentation unique (SSP) ou du modèle « acheter-expédier-payer ». Le document BRS doit inclure des éléments de données normalisés qui permettent une collaboration entre les plateformes et, si les données sont enregistrées à l'aide de dispositifs IoT, un système complètement intégré pour les échanges de données basé sur l'utilisation d'API partagées − qui sont, à leur tour, basées sur des normes. En outre, les données obtenues par les dispositifs IoT devraient aussi être conformes aux exigences de suivi des ressources pour le mappage des points de données tels que les lieux, les entreprises ou les différentes parties prenantes.

29. Le partage efficace des données est important pour le bon fonctionnement des chaînes d'approvisionnement logistiques, car les parties prenantes participant aux transactions sont multiples et les chaînes d'approvisionnement, mondiales et diverses. De nombreux conteneurs et dispositifs intelligents sont déjà utilisés, mais il n'existe actuellement aucune norme mondiale pour recenser et communiquer de manière cohérente l'ensemble des données recueillies par les conteneurs intelligents.

30. Le CEFACT-ONU a déjà créé un document BRS conteneur intelligent qui est la première norme officielle détaillant les éléments des données du conteneur intelligent. Il est important d'adhérer à ces normes car les différentes parties prenantes ont grandement besoin que les conteneurs intelligents soient plus largement adoptés. Dans ce contexte, l'utilisation de dispositifs IoT, associée à des normes, favorise une adoption accrue et garantit l'interopérabilité.

31. L'IoT peut également être déployée dans les portails de présentation unique (SSP), car la normalisation du flux de données en est un élément important, qui offre le moyen de

relier les autorités nationales et les entreprises dans le commerce transfrontalier[8]. L'un des principaux objectifs de tout SSP est de permettre et de faciliter la déclaration précise des données aux autorités de contrôle des frontières qui les utiliseront pour délivrer des autorisations et gérer les risques aux frontières. La réussite de la mise en œuvre des SSP repose sur l'utilisation d'échanges de messages et d'informations dans une structure et un format convenus, de sorte que les deux parties puissent lire et comprendre les données grâce à l'interopérabilité sémantique[9]. Traditionnellement, l'interopérabilité sémantique est fondée sur l'élaboration d'un modèle de référence commun relatif aux données servant de fondement logique au flux des informations utilisées dans le commerce transfrontalier.

32. L'harmonisation des données est un élément important s'agissant d'atteindre les objectifs des SSP, qui va de pair avec l'élimination des redondances, de l'ambiguïté des données et des doublons, ce qui exige, pour une exécution efficace, la mise en correspondance des exigences en matière de données des documents avec les normes internationales du commerce transfrontalier[10]. Le partage normalisé des informations, soutenu par le déploiement de systèmes IoT et de systèmes de chaînes de blocs utilisant des données normalisées, peut contribuer à atteindre les objectifs d'un SSP s'il est intégré dans le cadre des processus définis dans un BRS et un RSM. Les documents tels que les permis, les certifications et les déclarations en douane peuvent être conservés numériquement une fois que les principales données ont été obtenues à l'aide de dispositifs IoT et peuvent être stockés sur une chaîne de blocs afin de garantir leur intégrité permanente. Mais pour atteindre cet objectif, il faut établir des formats d'échange de messages et des interfaces appropriés et normaliser les éléments de données, en tenant compte du besoin de transparence et de respect de la vie privée des utilisateurs, conformément au Règlement général sur la protection des données de l'Union européenne (RGPD) et à d'autres législations. L'utilisation de systèmes IoT robustes ainsi que de chaîne de blocs à autorisation peut fournir l'infrastructure souhaitée pour atteindre les objectifs d'un SSP.

33. Dans le modèle « acheter-expédier-payer », il faut en faire plus pour réaliser le plein potentiel du modèle et du déploiement de l'IoT. Lorsqu'il y a des lacunes dans le modèle existant, les normes doivent répondre aux besoins suivants[11] :

- Appui pour une plus grande visibilité et un meilleur suivi de la chaîne d'approvisionnement grâce à une documentation et une normalisation détaillées des changements d'état subis par les entités du processus « acheter-expédier-payer » afin de suivre les flux de données granulaires et de les relier à des événements de niveau supérieur plus pertinents ;
- Appui à la santé et au bien-être des animaux par des normes relatives aux processus et aux données pour l'échange et l'utilisation de données IoT pertinentes (par exemple, sur les températures dans les wagons à bestiaux, l'état d'hydratation des animaux) ;
- Appui au suivi et à la traçabilité de la logistique et satisfaction des besoins concernant la réglementation par des BRS/RSM qui indiquent l'utilisation de données IoT (par exemple à partir de dispositifs de surveillance fixés sur les marchandises ou les conteneurs) ;
- Identification de nouvelles possibilités dans le cadre du modèle « acheter-expédier-payer » pour les processus qui utilisent les données IoT dans les pipelines de données à des fins d'établissement réglementaire de rapports, de fabrication, de planification, de gestion des matériaux, de financement des commandes et de marchés publics.

34. Souvent, un manque de transparence dans l'échange de données entre les différentes parties prenantes du commerce transfrontalier mondial constitue un obstacle à la réalisation

[8] CEFACT-ONU, recommandation nº 37 : Portail de présentation unique (ECE/TRADE/447) (2019). Disponible à l'adresse https://unece.org/fileadmin/DAM/trade/Publications/ECE_TRADE_447E_CF-Rec37.pdf.

[9] Ibid.

[10] https://tfig.unece.org/FR/contents/data-harmonization.htm.

[11] CEE, « Programme de travail du CEFACT-ONU 2019-2020 » (ECE/TRADE/C/CEFACT/2019/21) (2019). https://unece.org/fileadmin/DAM/cefact/GuidanceMaterials/PoW_2019-2020_E.pdf.

de tous les avantages des chaînes d'approvisionnement numériques. La technologie de la chaîne de blocs assure la transparence et un haut niveau de fiabilité parce qu'elle enregistre et stocke les données de manière sécurisée à l'aide de la cryptographie. Une fois que les données IoT sont obtenues à partir de l'environnement du conteneur, d'autres informations, telles que l'emplacement/le positionnement du conteneur, peuvent être obtenues (également à l'aide de l'IoT) et ajoutées au dossier d'expédition enregistré sur une chaîne de blocs.

35. L'intégration des données collectées à l'aide de l'IoT pendant les mouvements de l'expédition sur la base des normes relatives aux données BRS/RSM est essentielle pour améliorer l'efficacité des chaînes d'approvisionnement et passer au commerce transfrontalier sans papier. Une normalisation plus poussée de ces processus, associée à l'enregistrement des données sur des chaînes de blocs, offrira une plus grande visibilité et un meilleur accès des données (via l'interopérabilité) pour les organismes de réglementation aux frontières, ce qui leur permettra d'accélérer les processus commerciaux. En un mot, l'adoption de l'IoT ainsi que de la technologie de la chaîne de blocs dans les normes relatives aux données BRS et RSM renforcera considérablement l'efficacité des chaînes d'approvisionnement numériques, car la normalisation augmentera le nombre de données recueillies et leur utilisation. Elle permettra aussi d'améliorer l'analyse des données et la prise de décisions en permettant aux moteurs d'intelligence artificielle d'utiliser des données normalisées provenant de sources multiples.

V. Questions relatives à la cybersécurité

36. L'IoT désigne le réseau numérique croissant de liens qui connectent des appareils et des capteurs afin de faciliter le transfert de données sur Internet sans intervention extérieure. Dans cet environnement numérique florissant, alors que les transferts de données basés sur la technologie deviennent de plus en plus applicables à l'échelle mondiale, le commerce international continue de se développer par-delà les frontières. La numérisation par l'IoT a commencé à transformer le paysage du commerce, notamment dans le contexte transfrontalier. L'IoT favorise la simplification des documents commerciaux électroniques par la collecte automatique de données essentielles, qui, associée à la technologie de la chaîne de blocs, peut accélérer les procédures d'exportation et d'importation. La possibilité de suivre les expéditions via l'IoT a déjà permis d'accroître l'efficacité des transports[12], tandis que l'authentification électronique peut faciliter la vérification des transactions en ligne[13]. Comme l'indiquent les tendances observées, l'imbrication de l'Internet et des dispositifs informatiques fera désormais partie intégrante de l'activité économique. Pour la seule année 2020, on estime que les ventes mondiales du commerce électronique ont atteint une valeur de 26 700 milliards de dollars des États-Unis[14], et on prévoit que le commerce électronique transfrontalier représentera 22 % de toutes les ventes de commerce électronique en 2022 (contre 15 % en 2016[15]). En outre, on prévoit que 500 milliards d'appareils seront connectés

[12] Organisation mondiale du commerce, *Rapport sur le commerce mondial 2018 : L'avenir du commerce mondial : comment les technologies numériques transforment le commerce mondial et le commerce*, (2018), p. 71, 72 et 78. Disponible sur https://www.wto.org/english/res_e/publications_e/world_trade_report18_e.pdf (consulté le 24 mai 2022).

[13] Maria Ptashkina, « Facilitation 2.0: E-Commerce and Trade in the Digital Age » (RTA Exchange, Centre international pour le commerce et le développement durable (ICTSD) et Banque interaméricaine de développement (BID), (2018), p. 9. Disponible sur https://e15initiative.org/wp-content/uploads/2015/09/rta_exchange_-_ptashkina_-_facilitation_2.0_-_e-commerce_-_ptashkina_0.pdf (consulté le 24 mai 2022).

[14] Conférence des Nations Unies sur le commerce et le développement (CNUCED), « Le commerce électronique mondial atteint 26 700 milliards de dollars, le COVID-19 stimule les ventes en ligne » (3 mai 20219). Disponible sur https://unctad.org/fr/news/le-commerce-electronique-mondial-atteint-26-700-milliards-de-dollars-le-covid-19-stimule-les (consulté le 24 mai 2022).

[15] Statista.com, « Cross-border e-commerce as share of total e-commerce worldwide in 2016 and 2022 », disponible sur https://www.statista.com/statistics/867991/cross-border-e-commerce-share-world/ (consulté le 24 mai 2022).

à l'Internet d'ici à 2030[16], alors que les vulnérabilités liées au déploiement des appareils connectés restent largement négligées[17]. Les problèmes de compatibilité et d'interopérabilité du matériel et des logiciels (faute d'une conception soucieuse de la sécurité) risquent de s'exacerber en raison de l'augmentation exponentielle des appareils IoT connectés[18]. Les entreprises opérant fréquemment au-delà des frontières pour réduire les coûts du commerce, les documents et les données commerciales sont échangés entre plusieurs réseaux situés dans différents pays[19]. Cette évolution a accru les menaces à la cybersécurité liées à l'afflux de données commerciales transfrontalières[20].

37. Les dispositifs IoT interconnectés peuvent permettre l'accès à de vastes volumes de données dans divers secteurs où il existe un sérieux potentiel d'utilisation abusive. Si les écosystèmes de l'IoT doivent favoriser le commerce, leur ouverture, leur stabilité, leur sécurité et leur fiabilité doivent être des conditions préalables à leur utilisation dans le commerce international[21]. Étant donné que le commerce international et la dépendance à l'égard de l'IoT ne feront que croître et s'amplifier, les préoccupations des entreprises devraient aller au-delà des pertes monétaires potentielles pour inclure les dommages à la réputation.

38. Aux fins du présent rapport, nous partons du principe que l'élaboration d'un ensemble complet de normes de cybersécurité dans le cadre d'une collaboration public-privé pourrait faciliter la sécurisation des échanges transfrontaliers.

A. Normes relatives à la cybersécurité : les incidences plus larges

39. Les cybermenaces prolifèrent dans un environnement d'innovation et de croissance technologiques ; cependant, il n'existe pas encore de définition universellement acceptée de ce que devraient être les normes de cybersécurité. Aujourd'hui, ces normes peuvent prendre la forme de lois, de règles, de principes, de lignes directrices, de meilleures pratiques, de systèmes de certification, de spécifications techniques et/ou d'autres cadres élaborés par des entités publiques, privées ou à but non lucratif[22].

[16] CISCO, « At-a-Glance: Internet of Things: Connected Means Informed » (2016). Disponible sur https://emarsonindia.com/wp-content/uploads/2020/02/Internet-of-Things.pdf (consulté le 6 mars 2020).

[17] EY, « Cybersecurity and the Internet of Things » (2015), p. 10 et 11. Disponible sur https://pdf4pro.com/amp/view/ey-cybersecurity-and-the-internet-of-things-567613.html (consulté le 24 mai 2022).

[18] Forum économique mondial, « Global Risks Report 2020 », *Insight Report, 15th Edition* (2020), p. 62. Disponible sur http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf (consulté le 24 mai 2022) ; Siddiqui, F. M., M. Hagan et S. Sezer, « Embedded Policing and Policy Enforcement Approach for Future Secure IoT Technologies », *Living in the Internet of Things : Cybersecurity of the IoT-2018*, (document de conférence). p. 5. Disponible sur https://pureadmin.qub.ac.uk/ws/portalfiles/portal/153474397/Final_Paper_Submitted.pdf (consulté le 24 mai 2022).

[19] Commission économique et sociale pour l'Asie et le Pacifique (CESAP), « Mechanism for cross-border mutual recognition of trade-related data and documents in electronic form » (2019). Document de séance pour la cinquième réunion du Groupe directeur intergouvernemental intérimaire sur la facilitation du commerce transfrontalier sans papier par les groupes de travail juridique et technique, p. 6. Disponible à l'adresse https://www.unescap.org/sites/default/files/B1900234.pdf (consulté le 24 mai 2022).

[20] Joshua P. Meltzer, « Cybersecurity and digital trade: What role for international trade rules? », (Brookings Institution, 2019), p. 2. Disponible sur https://www.brookings.edu/wp-content/uploads/2019/11/Cybersecurity-and-digital-trade_final-11.20.pdf (consulté le 24 mai 2022).

[21] Neha Mishra, « International Trade, Internet Governance and the Shaping of the Digital Economy » (UNESCAP, 2017) ARTNeT Working Paper Series No 168. Disponible à l'adresse https://www.unescap.org/sites/default/files/B1900234.pdf (consulté le 24 mai 2022).

[22] Brass, I., et al. « Standardising a Moving Target: The Development and Evolution of IoT Security Standards » (juin 2018) *Living in the Internet of Things: Cybersecurity of the IoT − 2018*, Conference Paper, p. 2. Disponible sur https://www.researchgate.net/publication/325436966_Standardising_a_Moving_Target_The_Development_and_Evolution_of_IoT_Security_Standards (consulté le 24 mai 2022).

40. Aux États-Unis, la loi californienne sur la protection de la vie privée des consommateurs et, en Europe, le Règlement général sur la protection des données de l'Union européenne ciblent l'utilisation et la collecte des données personnelles (qui incluent les données personnelles recueillies par les dispositifs IoT) plutôt que de traiter spécifiquement les aspects de sécurité de l'IoT. Cependant, depuis 2017, le Sénat des États-Unis a introduit et examiné la Loi sur l'amélioration de la cybersécurité de l'IoT, qui impose à l'Institut national des normes et de la technologie (NIST) de prendre des mesures précises pour accroître la cybersécurité des dispositifs IoT[23]. De même, la Commission européenne a défini un cadre de certification volontaire en matière de cybersécurité (fondé sur des niveaux d'assurance) visant à accroître la fiabilité et la sécurité des dispositifs IoT en 2018[24]. Ces évolutions de la réglementation mettent l'accent sur la nécessité de mettre en œuvre des mécanismes de cybersécurité qui renforcent la fiabilité des écosystèmes IoT, ce qui, à son tour, améliore confiance dans le commerce international. La gestion des menaces et l'atténuation des risques vont nécessairement de pair avec la conception d'un cadre complet permettant d'élaborer des politiques capables de sécuriser largement les interfaces entre les produits, les processus et les technologies avec les meilleures pratiques de conformité. L'établissement de normes de cybersécurité est crucial pour toute entreprise qui souhaite prospérer.

41. La détermination de la forme et du fond des résultats attendus quant à la sécurité est fondamentale pour l'assurance en matière de cybersécurité. Au départ, il peut être difficile de concevoir un ensemble commun de normes pour toutes les applications IoT des différentes juridictions[25]. Cela n'est pas surprenant si l'on considère que les organismes de normalisation ont leurs propres priorités et critères lorsqu'ils évaluent les risques liés à la cybersécurité dans les écosystèmes IoT. Cela dit, l'adoption des principes de sécurité dès la conception en tant qu'exigence de base (c'est-à-dire l'intégration de fonctions de sécurité dans les dispositifs IoT dès la phase de conception) pourrait être nécessaire pour résoudre les problèmes urgents d'interopérabilité[26].

42. Pour concevoir un cadre de normes relatives à la cybersécurité, il est important de commencer par déterminer les éléments qui doivent être sécurisés[27]. Faut-il sécuriser le dispositif, le système, le processus, l'organisation, les données de l'IoT ou les personnes au sein de l'écosystème IoT ? Une fois ces éléments déterminés, les organismes de normalisation peuvent définir la portée de leurs propres principes de sécurité dès la conception et décider des aspects de la sécurité de l'IoT qui doivent être inclus dans leurs impératifs de sécurité de base/minimum. Par exemple, le Centre national japonais de préparation et de stratégie face aux incidents en matière de cybersécurité (NISC) considère que la sécurisation des systèmes IoT dans les phases de conception, de développement et d'exploitation fait partie de ses principes de sécurité dès la conception[28]. Une approche

[23] Congrès américain, « S.734 − Internet of Things Cybersecurity Improvement Act of 2019 » cent-seizième Congrès (2019-2020). Disponible sur https://www.congress.gov/bill/116th-congress/senate-bill/734 (consulté le 24 mai 2022).

[24] Commission européenne, « Le cadre de certification de l'UE en matière de cybersécurité ». Disponible sur https://digital-strategy.ec.europa.eu/fr/policies/cybersecurity-certification-framework (consulté le 24 mai 2022).

[25] Brass, I., et al. p. 6.

[26] HM Government (Royaume-Uni), « Internet Safety Strategy-Green Paper 2017 » (octobre 2017) p. 11. Disponible à l'adresse https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/650949/Internet_Safety_Strategy_green_paper.pdf (consultée le 24 mai 2022). À l'évidence, les autorités britanniques sont en faveur du principe d'intégration de la sécurité dès la conception, comme en témoignent les publications du Ministère du numérique, de la culture, des médias et du sport relatives au « Secure by Design : Improving the cyber security of consumer Internet of Things Report » et du voluntary « Code of Practice for Consumer IoT Security » en 2018 (ces deux publications étant toutefois orientées vers la protection des intérêts des consommateurs lors de l'utilisation de dispositifs IoT).

[27] Carr, M., et al, « Standards, Governance, and Policy Stream − Governance and Policy Cooperation on the Cyber Security of the Internet of Things » (PETRAS Internet of Things Research Hub, (27 mars 2018) p. 22 et 23. Disponible sur https://discovery.ucl.ac.uk/id/eprint/10063234/1/Carr_Report_Global-governance-of-the-Internet-of-Things-Report-PDF.pdf (consulté le 24 mai 2022).

[28] NISC (Japon), « General Framework for Secure IoT Systems » (26 août 2016), p. 1. Disponible sur https://www.nisc.go.jp/eng/pdf/iot_framework2016_eng.pdf (consulté le 24 mai 2022).

globale de la définition de ces principes est essentielle compte tenu de l'effet considérable et croissant que les écosystèmes IoT ont sur la facilitation du commerce international tout au long des chaînes d'approvisionnement.

43. Le développement mondial d'exigences de base en matière de sécurité est encore à l'état embryonnaire, la marge de manœuvre concernant la définition des protocoles d'action préventive et corrective étant extrêmement vaste. La littérature existante a noté une tendance de plus en plus convergente en faveur de l'élaboration d'un ensemble de spécifications minimales pour la sécurité de l'IoT aux États-Unis et dans l'UE[29] ; cependant, l'élaboration des exigences de base la plus récente et en cours présente un tableau légèrement différent. À partir de la version préliminaire de ses exigences de base fondamentales, le NIST met davantage l'accent sur la sécurisation de l'IoT au niveau des dispositifs[30], tandis qu'à l'inverse, l'Agence européenne pour la cybersécurité (ENISA) approuve les principes de sécurité dès la conception et de respect de la vie privée dès la conception (protection des données) tout au long du cycle de vie des dispositifs IoT et de leur écosystème[31]. Les développeurs de systèmes IoT sont également encouragés à donner la priorité à la surveillance de la sécurité et à l'analyse de l'efficacité.

44. L'élaboration et la mise en œuvre des normes de l'IoT présentent des difficultés intrinsèques. La technologie de l'IoT et celle des cyber-pirates ne cessent d'évoluer. Dans le même temps, l'élaboration de normes internationales peut prendre des années. Par exemple, il faut en moyenne trois ans pour élaborer une norme ISO, de la première proposition à la publication finale[32]. Cela signifie que les organismes de normalisation sont dans une course constante pour suivre l'évolution rapide du domaine de la cybersécurité. Par ailleurs, un nombre croissant d'associations d'entreprises ont été encouragées à élaborer leurs propres normes afin de combler ce vide. Ainsi, les exécutants font face à des difficultés pour évaluer

[29] Brass et al. (n. 12) p. 3. Les auteurs ont noté une certaine récurrence pour ce qui était des exigences minimales de sécurité de l'IoT dans les documents du NIST, notamment ceux concernant l'IoT : au niveau des appareils, ces exigences pouvaient inclure la divulgation des vulnérabilités, la mise à niveau et la gestion du cycle de vie des services. Au niveau du système, elles comprenaient l'authentification, l'autorisation, les contrôles d'accès, la gestion des clés cryptographiques et la gestion de l'intégrité.

[30] NIST, « Considerations for a Core IoT Cybersecurity Capabilities Baseline », projet de document (2019), p. 5 à 9. Disponible sur https://www.nist.gov/system/files/documents/2019/02/01/final_core_iot_cybersecurity_capabilities_baseline_considerations.pdf (consulté le 24 mai 2022). Les exigences minimales de sécurité au niveau des appareils (que le NIST suggère d'inclure dans son état de référence) comprennent notamment l'identification physique et logique de l'appareil ; la mise à jour du logiciel et du micrologiciel de l'appareil ; la possibilité de modifier en toute sécurité sa configuration ; la possibilité de contrôler son accès local et à distance ; le recours à la cryptographie. Étant donné la difficulté de vérifier les principes de conception et le coût probablement élevé de la mise en œuvre, le NIST suggère d'exclure la pratique de la conception et de la configuration de l'appareil connecté de son référentiel de capacités de cybersécurité IoT de base. Voir également NIST, « NISTIR 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risk » (2019) p. 11 et 12. Disponible sur https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8228.pdf (consulté le 24 mai 2022). Le NIST classe les risques de cybersécurité pour les appareils connectés en fonction de la sécurité de leur sécurité, de la sécurité des données et de la confidentialité. Il prend également en compte d'autres aspects essentiels d'atténuation des risques, notamment la gestion des actifs, la gestion des vulnérabilités, la gestion des accès, la détection des problèmes, la protection des données et la gestion des flux d'informations. Certains de ces aspects se recoupent avec les mesures de sécurité minimum énumérées dans les recommandations de sécurité de base de l'ENISA (voir ci-dessous).

[31] Agence européenne pour la cybersécurité (ENISA), « Baseline Security Recommendations for IoT in the context of critical information infrastructures » (novembre 2017), p. 46 à 52. Disponible sur https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot/at_download/fullReport (consulté le 24 mai 2022). L'ENISA classe les mesures de sécurité de base de l'IoT dans trois catégories : les mesures relatives aux politiques ; les mesures relatives à l'organisation, aux personnes et aux processus ; les mesures non techniques. Certaines des mesures de sécurité qui se recoupent avec celles du NIST américain sont la gestion des actifs, la gestion des vulnérabilités et/ou des incidents de sécurité, le contrôle d'accès, la mise à jour sécurisée des logiciels/micrologiciels, la cryptographie, la protection des données et la conformité, etc.

[32] ISO, « Developing Standards » https://www.iso.org/developing-standards.html (consulté le 24 mai 2022).

et suivre l'évolution des normes, et il existe un risque sérieux que des normes se chevauchent[33]. Autre conséquence, si des institutions publiques telles que l'ENISA en Europe ou le NIST aux États-Unis peuvent émettre des recommandations utiles, celles-ci risquent de ne pas suffire à garantir la cybersécurité de l'IoT compte tenu du rôle sans cesse croissant des écosystèmes IoT dans la facilitation du commerce international.

45. La collaboration public-privé dans l'élaboration de normes de cybersécurité est de plus en plus souvent perçue comme une option viable. L'écosystème IoT présente un éventail diversifié de domaines d'application. Les parties prenantes de chaque secteur peuvent donc coopérer et élaborer des normes de cybersécurité IoT spécifiques au secteur et fondées sur un consensus[34]. Par exemple, la recommandation de l'Organisation de coopération et de développement économiques (OCDE) sur la sécurité numérique encourage la coordination et la collaboration entre toutes les parties prenantes (y compris les États et le secteur privé) qui dépendent de « l'environnement numérique pour tout ou partie de leurs activités économiques »[35]. En établissant une comparaison avec le secteur juridique, l'Association internationale du barreau, par exemple, a établi un dialogue entre de multiples parties prenantes de la profession afin d'élaborer une liste de recommandations concernant les meilleures pratiques, pour aider les cabinets d'avocats à se protéger contre les cybermenaces[36]. Dans le cadre de ce processus, des praticiens, des experts juridiques, des professionnels de l'informatique et des communications ainsi que des consultants en cybersécurité ont participé à l'élaboration des lignes directrices relatives à la cybersécurité visant à renforcer l'infrastructure technologique, les processus organisationnels et les politiques de formation du personnel des cabinets juridiques[37].

46. Pour que l'écosystème IoT joue un rôle central dans le commerce, il est important de collaborer avec des experts du secteur et de réunir différentes parties prenantes (notamment les développeurs IoT, les experts du commerce et les spécialistes de la cybersécurité) afin de déterminer conjointement ce qui doit être sécurisé, et comment le faire, afin de développer encore le commerce mondial.

B. Rôle des accords commerciaux et du commerce électronique

47. Il convient de noter que c'est seulement depuis peu que les accords commerciaux internationaux comportent des chapitres consacrés expressément aux questions relatives au commerce électronique, comme le montre la publication intitulée *Facilitation 2.0 : E-Commerce and Trade in the Digital Age*. Ces questions concernent notamment la restriction des flux de données numériques et les problèmes de cybersécurité. En 2007, l'Union internationale des télécommunications (UIT) a lancé le Programme mondial cybersécurité, qui constitue un cadre pour la coopération internationale des États membres destiné à renforcer la confiance et la sécurité dans le contexte des nouvelles technologies. La Commission des Nations Unies pour le droit commercial international (CNUDCI) a joué un rôle important dans la facilitation des échanges internationaux en modernisant les règles du commerce mondial. Sa loi type sur les documents électroniques transférables (MLETR) s'appuie sur les principes d'équivalence fonctionnelle et de neutralité technologique qui sous-tendent tous les textes de la CNUDCI sur le commerce électronique. La liste des critères d'évaluation de la norme générale de fiabilité des documents électroniques transférables établie à l'article 12 du chapitre III mentionne expressément la « sécurité du matériel et des logiciels ». La précision est importante car cette sécurité a un impact direct sur la fiabilité de

[33] Brass et al., p. 6.

[34] OCDE, *Gestion du risque de sécurité numérique pour la prospérité économique et sociale* : recommandation de l'OCDE et son document d'accompagnement (Éditions OCDE, Paris, 2015). Disponible sur https://www.oecd.org/fr/sti/ieconomie/digital-security-risk-management.htm (consulté le 24 mai 2022).

[35] Ibid., p. 8.

[36] Association internationale du barreau (IBA), « Cybersecurity Guidelines by the IBA's Presidential Task Force on Cybersecurity » (2018), p. 4. Disponible sur https://dokumen.tips/documents/cybersecurity-guidelines-hspi-attacking-unsecured-wi-fi-connections-eg-public.html?page=1 (consulté le 24 mai 2022).

[37] Ibid., p. 6 à 21.

la méthode utilisée par les pays pour faciliter le commerce numérique transfrontalier, en particulier lorsque les données sont extraites des écosystèmes IoT.

48. En règle générale, les pays peuvent adopter des normes internationales ou consensuelles pour conclure des accords commerciaux afin de soutenir « l'élaboration d'approches de la cybersécurité cohérentes au niveau mondial et présentant le moins de restrictions commerciales possibles »[38]. Toutefois, les parties qui négocient les accords doivent d'abord se mettre d'accord sur les normes ou les infrastructures de cybersécurité que chacune d'entre elles juge mutuellement acceptables ou équivalentes dans son propre cadre réglementaire/législatif en matière d'IoT, ce qui, très souvent, est un point litigieux. En outre, il ne faut pas sous-estimer les tensions qui entourent les questions de sécurité nationale et de cybersécurité, car l'imbrication des nombreux intérêts entraîne nécessairement un examen attentif et constitue un véritable exercice d'équilibre. Les litiges en cours concernant le commerce international et la propriété des données de l'IoT, l'application du droit international dans l'espace numérique et le désir des États de protéger leur souveraineté continueront de créer des goulets d'étranglement importants s'agissant d'élaborer un cadre de normes de cybersécurité au niveau mondial.

VI. Conclusions et propositions concernant les travaux futurs du CEFACT-ONU

49. La technologie IoT va connaître un développement exponentiel dans un avenir proche, avec la prolifération de systèmes de communication tels que ceux qui utilisent la technologie 5G. Compte tenu de ce contexte, le CEFACT-ONU est idéalement placé pour piloter l'élaboration de nouvelles spécifications techniques visant à renforcer l'utilisation de l'IoT dans le commerce et, dans le même temps, à améliorer la capacité qu'ont les normes actuelles de répondre aux besoins de l'évolution de l'environnement technologique.

A. Interopérabilité

50. L'évolution de l'IoT a conduit différents fabricants et développeurs d'applications à adopter des technologies, des normes et des protocoles de communication différents pour recueillir et échanger des informations. À mesure que l'utilisation de l'IoT se développe, il va devenir de plus en plus nécessaire de garantir l'interopérabilité afin que les différents dispositifs et systèmes IoT puissent échanger des informations entre eux.

51. Le CEFACT-ONU peut jouer un rôle important dans ce domaine, en développant et en encourageant l'utilisation de normes concernant les données pour l'interopérabilité de l'IoT.

B. Découverte de ressources

52. Dans le contexte du commerce transfrontalier, l'utilisation de l'IoT générera des données qui pourraient être saisies dans un système, traitées dans un autre et stockées dans un troisième, tous ces systèmes pouvant être en ligne et relever de juridictions diverses. Les éléments clefs tels que les informations sur le dispositif IoT utilisé pour recueillir les données ou les événements ou encore les éléments de données dans le cadre d'un flux d'événements doivent pouvoir être découverts si l'on veut assurer la transparence et la visibilité dans l'ensemble de la chaîne d'approvisionnement.

53. Comme dans le cas de la technologie de la chaîne de blocs, l'IoT offre aussi l'occasion au CEFACT-ONU de jouer un rôle essentiel pour combler cette lacune et élaborer des spécifications permettant à divers systèmes et plateformes de découvrir des ressources telles que des informations relatives à l'identité ou aux événements.

[38] https://www.brookings.edu/research/cybersecurity-and-digital-trade-getting-it-right/.

C. Cadre législatif et réglementaire

54. La nature dynamique des cybermenaces exige l'adoption d'une logique proactive pour faire face à ces risques et les atténuer. La tendance récente qui consiste à intégrer des fonctions de cybersécurité dans les dispositifs et logiciels IoT, selon les principes de la sécurité dès la conception, est un pas dans la bonne direction. Il est essentiel d'adopter une approche de collaboration multipartite, assortie d'un dialogue permanent entre les parties prenantes des sphères publique et privée, pour déterminer la meilleure forme et le meilleur contenu des normes de sécurité de l'IoT. Une collaboration approfondie entre les organismes de normalisation de l'IoT pourrait contribuer efficacement à l'élaboration d'un ensemble complet de normes de cybersécurité pour les écosystèmes de l'IoT. En définitive, le commerce et la cybersécurité sont deux rouages du mécanisme de l'IoT. En réduisant les risques relatifs à la cybersécurité au sein des écosystèmes IoT grâce à l'utilisation de normes, on contribuerait grandement à faciliter un commerce international sécurisé.

D. Besoins en données des applications de l'Internet des objets

55. Dans le cadre du projet sur les conteneurs intelligents, la CLL du CEFACT-ONU a été enrichie par l'ajout de 120 nouveaux éléments de données, l'objectif étant la prise en compte de l'utilisation de dispositifs IoT dans les conteneurs. Il ne s'agit que d'une application IoT ; il est possible de collaborer avec des développeurs d'applications dans d'autres domaines pour recenser les données IoT qui doivent être définies, mais qui ne sont pas encore incluses dans les normes actuelles du CEFACT-ONU. Les systèmes IoT fonctionnant plutôt par l'envoi fréquent de rafales de petites données, il pourrait également être nécessaire de répondre à ce besoin dans le cadre de l'action de normalisation et d'harmonisation et de la poursuite du développement des BRS, du RSM et de la CCL.

56. L'utilisation de l'IoT ne fera qu'augmenter au fil du temps et interopérera également de plus en plus avec d'autres technologies émergentes telles que la technologie de la chaîne de blocs, l'intelligence artificielle, les technologies 5G et les plateformes d'API. Le CEFACT-ONU pourrait donc jouer un rôle important en collaborant avec les organismes de normalisation pour combler le fossé entre les normes existantes et tout ce qui pourrait être nécessaire pour accroître l'adoption de l'IoT dans les applications de facilitation du commerce.