Syntec NUMÉRIQUE

Position | Cybersécurité

Le chiffrement en cinq questions, une technologie indispensable - Les recommandations du Comité cybersécurité

Avec plus de 1500 entreprises adhérentes représentant les principaux acteurs et métiers des industries numériques, Syntec Numérique est le syndicat professionnel des entreprises de services du numérique, des éditeurs de logiciels et des sociétés de conseil en technologies. A ce titre, il est le porte-parole et acteur majeur de l'industrie numérique auprès de différents organismes institutionnels et des pouvoirs publics Français et Européen.

Syntec Numérique a créé un Comité cyberécurité coprésidé par Olivier Vallet (Sopra Steria) et Jean-Paul Alibert (T-systems France).

Synthèse des recommandations

- Le chiffrement doit devenir un standard incontournable pour la majorité des entreprises et doit être compris par les citoyens et les pouvoirs publics.
- Chaque utilisateur de numérique doit être sensibilisé à l'importance du chiffrement : le citoyen pour protéger ses données, les entreprises pour protéger leurs infrastructures et les secrets d'affaires, les pouvoirs publics pour éviter les attaques et s'en défendre.
- Le cercle vertueux sécurité/usage permet d'encourager la transformation numérique des entreprises françaises et de la société, stimule la compétitivité et le niveau d'activité, stimule l'innovation des prestataires de cybersécurité.
- Le chiffrement permet la circulation des données de manière sûre. Il est un pilier du marché unique numérique européen.
- L'investissement dans le chiffrement ne peut être retardé : les industriels doivent développer des solutions efficaces et qui s'adaptent aux nouvelles techniques d'attaques.
- Les entreprises doivent investir dans des solutions de chiffrement à hauteur de leur activité à protéger. Sécuriser les actifs de l'entreprise en amont constitue un bon réflexe, moins coûteux que réparer les dommages liés à une attaque.
- Les produits de chiffrement doivent être neutres, non intrusifs, simples à utiliser, fiables. C'est à ce prix que la confiance des utilisateurs sera acquise.
- Les pouvoirs publics doivent encourager le chiffrement et ne pas chercher à l'affaiblir.
- Ils doivent renforcer la coopération judiciaire entre Etats membre de l'UE et la coopération entre acteurs publics et privés. L'ANSSI doit jouer un rôle moteur dans cette coopération.
- Le cadre légal du chiffrement est stabilisé et ne nécessite pas une surabondance de textes contradictoires. Les législations doivent être harmonisées pour faciliter la lutte contre les nouvelles formes d'attaque.

Position | Cybersécurité

Introduction

Un des composants clés de la confiance numérique est le chiffrement des données.
Le chiffrement permet la protection des données sensibles, soit stockées, soit en mouvement (communicantes). Il est une nécessité notamment pour tout système sécurisé de e-commerce ou de communication digitale (e-mail, voix ...).

Avertissement : La présente fiche est rédigée en tenant compte de l'état des connaissances technologiques et réglementaires actuelles. En effet, les techniques de chiffrement et de déchiffrement des données évoluent sans cesse. De même, les techniques doivent s'adapter à la puissance croissante des ordinateurs qui conduit à utiliser des moyens de plus en plus lourds pour chiffrer les données et les protéger.

Quoi ?

Le chiffrement est l'outil qui permet de sécuriser l'information dans notre univers numérique.
Le chiffrement est un procédé, vieux de plusieurs millénaires, qui consiste à encoder l'information de sorte à ce que seul son destinataire véritable puisse y accéder.

Comment ?

Dans sa forme la plus basique, l'opération de chiffrement consiste à prendre un message en clair et à le « brouiller » de telle sorte que seuls les destinataires désignés puissent en lire le contenu [1].

Dans sa forme moderne, le chiffrement s'appuie sur un mécanisme cryptographique – utilisant des algorithmes mathématiques sophistiqués – impliquant la connaissance d'un secret. Sans la connaissance de ce secret, il est quasiment impossible à une personne d'accéder aux données sous leur forme initiale [2].

[1] Selon le CNNum, « *le chiffrement est une méthode qui consiste à protéger des données ou des communications en les rendant illisibles de l'extérieur et déverrouillables par une clé* ». Tribune « chiffrement et lutte contre le terrorisme : attention à ne pas se tromper de cible ». Tribune publiée dans le Monde du 22 août 2016.
[2] Les méthodes de chiffrement sont dites à « clé symétriques » (l'auteur du message et le destinataire du message partagent le même secret : le mot de passe) ou « clés asymétriques » (l'auteur du message possède une clé publique et le destinataire possède une clé privé pour déchiffrer le message).

Digital Europe a produit un exemple simple de chiffrement (Digital views on encryption, 15 July 2016) : Prenons la phrase suivante : « *The weather in Brussels is often cloudy* » comme un exemple pour créer un texte chiffré (« cypher ») avec une clé.

Nous pouvons prendre une date (31 March 2016, 310316) et écrire les chiffres sous la phrase :

The	*weather*	*in*	*Brussels*	*is*	*often*	*cloudy*
310	3163103	16	31031631	03	16310	316310

Pour transformer le texte en texte crypté, chaque lettre doit être décalée en arrière dans l'alphabet (ABCDEFGHIJKLMNOPQRSTUVWXYZ) du nombre d'espaces indiqué par le chiffre qui figure sous chaque lettre (exemple : T recule de trois lettres et devient Q). Le message chiffré devient le suivant :

QGE TDUQGEO HH YQUPRYIR IP NZNDN ZKIRCY

Pour déchiffrer le texte, le destinataire du message devra connaitre la clé (31032016) et le code de déchiffrage (décaler en arrière dans l'alphabet d'autant de lettres que le nombre). Tant que ces informations restent secrètes, le message reste inviolé.

Pourquoi ? Pour quels risques couverts ?

L'objectif du chiffrement est de garantir la confiance dans les données échangées, soit pendant leur transfert, soit lors de leur stockage dans la mémoire d'un système informatique d'un ordinateur ou de centres de données.
Le chiffrement est utilisé dans le but de protéger les données des entreprises, des personnes, des Etats considérées comme sensibles ou privées. Ainsi, par exemple :

- les entreprises chercheront à protéger un secret de fabrication,
- les Etats chercheront à protéger des données classifiées pouvant mettre en danger la sécurité de la Nation,
- les citoyens chercheront à protéger leurs données de santé ou des photographies.

En matière de vie privée, le chiffrement permet d'éviter le vol d'informations et protéger des personnes : dans le cas de vol de smartphone, au-delà de la perte de l'appareil, les données qui sont stockées ne pourront pas être accessibles.

Le chiffrement est indispensable pour assurer le commerce sur Internet, protéger certains aspects de la vie privée des citoyens, permettre des échanges sûrs. En cela, les entreprises du numérique ne peuvent pas être bridées dans la protection des données de leurs clients ou donneurs d'ordre.

Quels enjeux ?

Dans un monde largement numérisé, le chiffrement est devenu une pierre angulaire de la sécurité. Selon la CNIL, il contribue à faire de la cybersécurité le « *vecteur de confiance et d'innovation* » [3] des personnes et de l'économie.
La CNIL considère ainsi primordial de :

- protéger les personnes et leur vie privée afin de garantir leurs droits fondamentaux,
- protéger les systèmes d'information des entreprises et des États, car les atteintes à ces systèmes peuvent occasionner de graves préjudices économiques, politiques, ou en termes de sécurité publique,
- promouvoir l'essor de l'économie du numérique, au travers des notions de confiance et de sécurité, pour stimuler l'innovation et la croissance,
- maintenir la compétitivité des acteurs nationaux du domaine de la cybersécurité pour soutenir l'économie.

Pour les entreprises, le premier enjeu du chiffrement est de protéger les données sensibles. Il vise également à maintenir la confiance des utilisateurs dans la sécurité de la data.
Dès lors que les produits de sécurité sont fiables et ergonomiques, les utilisateurs verront dans ces produits la meilleure manière de sécuriser leurs systèmes. Si les systèmes sont sécurisés, les échanges seront démultipliés, engendrant un cercle vertueux et un multiplicateur d'échanges de données. Les usages numériques tiennent donc en grande partie dans la sécurité, avec un outil majeur : le chiffrement.

Le chiffrement joue un rôle dans la protection des libertés fondamentales et des grands principes de la démocratie, comme le droit à la protection de la vie privée et le droit à la liberté d'expression. Le Conseil des droits de l'homme des Nations Unies note que la cryptographie et l'anonymat sont deux outils à préserver afin de protéger ces deux droits fondamentaux. En matière de respect de la vie privée, le chiffrement peut servir à garantir ce droit énoncé par la Convention européenne des droits de l'homme et des libertés fondamentales (article 8). Ainsi, il peut limiter les risques d'écoutes et d'interception des conversations entre personnes.

[3] Cnil, « les enjeux de 2016 : quelle position de la Cnil en matière de chiffrement ? », 8 avril 2016, https://www.cnil.fr/fr/les-enjeux-de-2016-3-quelle-position-de-la-cnil-en-matiere-de-chiffrement.

Que faire cependant lorsque le chiffrement est utilisé dans un but malveillant, par exemple par des terroristes ? Pour assurer la protection des citoyens, les services de l'Etat peuvent procéder, après accord de la justice, à des écoutes de personnes suspectées de terrorisme. Si les communications sont chiffrées, il sera difficile, voire impossible d'accéder au contenu des conversations. De même, dans le cadre d'une enquête judiciaire, les services d'investigation peuvent procéder à la saisie d'un matériel informatique pour accéder aux données qui y sont stockées. Si le disque dur du matériel informatique est chiffré, il sera impossible d'accéder aux informations sans connaissance de la clé permettant son déchiffrement[4].

Pour contourner ces problèmes, les Etats peuvent avoir la tentation d'imposer aux fournisseurs de moyens cryptographiques de fournir les clés de déchiffrement - dans la mesure où elles seraient leur possession - ou de créer des portes dérobées dans leurs produits.
Sans nier la légitimité des inquiétudes des forces de l'ordre et des autorités de renseignement, il existe de nombreux arguments d'intérêt général s'opposant aux atteintes au système cryptographique :

- Les portes dérobées peuvent, en premier lieu, remettre en cause la confiance des utilisateurs et introduiraient une faille « volontaire » dans le produit qui pourrait être exploitée par des personnes malveillantes (problème de robustesse face à des attaques). L'ENISA (Agence européenne pour la sécurité des réseaux et des systèmes d'information) estime que les portes dérobées risquent de « *créer des vulnérabilités qui peuvent être à leur tour utilisées par les cybercriminels et les terroristes* ».

- Ensuite, l'affaiblissement du chiffrement ne permet pas de contrer le terrorisme. Il suffit aux criminels d'utiliser des solutions de chiffrement alternatives ou illégales (marché noir). Ils échapperont de toute manière aux contrôles des autorités.

- Par ricochet, ce sont les personnes ou les entreprises n'ayant rien à se reprocher qui subiront une dégradation de leur protection.

- Les technologies sont déjà en place et sûres. Attenter à leur intégrité les affaibliraient au préjudice du « *patrimoine informationnel des entreprises, de la stabilité de l'écosystème du numérique et à la protection de la liberté des personnes* » [5].

[4] Dans certains cas, il est possible de s'appuyer sur des faiblesses ou failles de protocoles ou algorithmes pour parvenir à déchiffrer les données par cryptanalyse, c'est-à-dire sans posséder la clé de déchiffrement mais souvent à la condition de disposer de puissance de calcul suffisante.
[5] Cnil, Ibid, 8 avril 2016, https://www.cnil.fr/fr/les-enjeux-de-2016-3-quelle-position-de-la-cnil-en-matiere-de-chiffrement.

Quelle règlementation pour l'utilisation de moyens de chiffrement et leur commerce ?

✓ Cadre général en France :

En France, la réglementation générale est issue des articles 29 et suivants de la loi pour la confiance dans l'économie numérique (« LCEN »)[6]. L'article 29 définit les moyens de cryptologie et les prestations afférentes :

« On entend par moyen de cryptologie tout matériel ou logiciel conçu ou modifié pour transformer des données, qu'il s'agisse d'informations ou de signaux, à l'aide de conventions secrètes ou pour réaliser l'opération inverse avec ou sans convention secrète. Ces moyens de cryptologie ont principalement pour objet de garantir la sécurité du stockage ou de la transmission de données, en permettant d'assurer leur confidentialité, leur authentification ou le contrôle de leur intégrité.
On entend par prestation de cryptologie toute opération visant à la mise en œuvre, pour le compte d'autrui, de moyens de cryptologie ».

La fourniture, l'importation, le transfert intracommunautaire et l'exportation d'un moyen de cryptologie sont soumis, sauf exception, à déclaration ou à demande d'autorisation auprès de l'ANSSI (article 30 III de la LCEN).

De même, la fourniture de prestations de cryptologie (concept qui n'est pas clair) doit être déclarée auprès des services du Premier ministre, donc l'ANSSI (article 31 de la LCEN).

Toute personne qui connait la clé chiffrée d'un message permettant de le déchiffrer doit donner l'information lorsque la police la demande dans une enquête[7] : « E*st puni de trois ans d'emprisonnement et de 270 000 euros d'amende le fait, pour quiconque ayant connaissance de la convention secrète de déchiffrement d'un moyen de cryptologie susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit, de refuser de remettre ladite convention aux autorités judiciaires ou de la mettre en œuvre, sur les réquisitions de ces autorités* […] *Si le refus est opposé alors que la remise ou la mise en œuvre de la convention aurait permis d'éviter la commission d'un crime ou d'un délit ou d'en limiter les effets, la peine est portée à cinq ans d'emprisonnement et à 450 000 € d'amende ».*

[6] https://www.legifrance.gouv.fr/eli/loi/2004/6/21/ECOX0200175L/jo#JORFARTI000001093765
[7] Article 434-15-2 du Code pénal – modifié par la loi n°2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale.

Dans le cadre de l'enquête pénale, les autorités judiciaires (procureur de la République, juge d'instruction, officier de police judiciaire, sur autorisation du procureur de la République ou du juge d'instruction, ou juridiction de jugement saisie de l'affaire) peuvent, d'autorité, déchiffrer les données cryptées lorsque l'enquête le nécessite, en se faisant assister par des tierces personnes (article 230-1 du Code de procédure pénale). Ces mêmes protagonistes peuvent demander le recours aux moyens de l'Etat soumis au secret de la défense nationale si la peine encourue est égale ou supérieure à deux ans d'emprisonnement.

Les autorités de renseignement peuvent de la même manière demander à tout prestataire de cryptologie la remise des clés de déchiffrement de leurs solutions dans les soixante-douze heures.

✓ Cadre spécifique :

La plupart des pays disposent de lois régulant le chiffrement, pour son usage et son « commerce » [8].
Un effort d'harmonisation des règles d'import / export des technologies « dual-use » ou « double usage » (le chiffrement n'est pas le seul concerné) a abouti à un ensemble de principes appelés « Wassenaar Arrangement » partagés par quarante et un pays, dont la France, les Etats-Unis, la Russie [9]. En résumé, cet accord permet l'exportation libre des systèmes de chiffrement jusqu'à un certain niveau de longueur de clés. Cet accord permet aussi aux individus qui voyagent à l'étranger de transporter avec eux des produits chiffrés à usage personnel.
En France, l'usage du chiffrement est libre, et l'importation et commercialisation de moyens de chiffrement sont soumis à déclaration ou autorisation par l'ANSSI [10]. Le Service des biens double usage (SBDU) est l'autorité compétente pour la délivrance des licences. Ce régime a été conçu pour éviter que des pays non amicaux puissent entrer en possession de techniques cryptographiques.
Aux Etats-Unis, l'usage, la création et la vente de moyens de chiffrement est libre, ainsi que l'importation. Par contre, l'exportation de moyens de chiffrement est très réglementée.
Dans l'Union Européenne, les moyens de chiffrement sont libres d'usage, mais sont soumis à des restrictions à l'exportation. L'export au sein de l'Union est entièrement libre, même si chaque pays a établi ses propres règles.
Il est à noter que l 'Union Européenne s'est opposée à créer une obligation légale de mettre sous « séquestre » toutes les clés. Il y a quelques années, les Etats-Unis ont également abandonné cette idée.

Il existe de nombreuses normes nationales et internationales relatives au chiffrement. Une bonne connaissance des lois et règlements en matière de chiffrement est longue à acquérir. C'est un handicap pour les entreprises prestataires de cybersécurité car elles peuvent être exposées à de fortes pénalités. Il

[8] Ce cadre règlementaire s'explique car le chiffrement est une technologie dite de « *dual-use* », c'est à dire à la fois d'usage militaire et commercial.
[9] http://www.wassenaar.org/
[10] http://www.ssi.gouv.fr/administration/reglementation/controle-reglementaire-sur-la-cryptographie/

est donc dans l'intérêt de la sécurité d'une part, et de l'innovation d'autre part de faire converger au niveau international les règlementations encadrant le chiffrement, en revendiquant le plus haut niveau de sécurité possible (donc éviter le nivellement par le bas). Il faut aussi renforcer l'information des entreprises sur l'environnement règlementaire du chiffrement, enjeu crucial compte-tenu du poids pris par les données dans l'économie mondiale.

Les recommandations du Comité Cybersécurité

- Les entreprises et leurs représentants doivent :

✓ Former au chiffrement

❖ Former les citoyens / utilisateurs

Une information du public doit être effectuée par les entreprises du secteur numérique.
Il est certain que les personnes ne connaissent pas l'impact et l'importance du chiffrement. Il convient de leur expliquer l'intérêt de chiffrer son ordinateur personnel ou d'effacer les données à la dixième tentative de craquage d'un iPhone.

❖ Former et responsabiliser les autres entreprises

Il est primordial de prendre conscience que des attaques peuvent toucher n'importe quelle entreprise, quel que soit son secteur d'activité, comme l'a récemment montré l'actualité.
Les entreprises doivent penser « analyse de risque » et « protection de l'information ».
Les premiers réflexes de protection, humains, organisationnels et technologiques, devraient être acquis par toute entreprise.
L'utilisation efficace du chiffrement nécessite une formation des utilisateurs, en particuliers des PME, à choisir des solutions de chiffrement reconnues et efficaces. Les utilisateurs devront également être formés aux aspects réglementaires et techniques du chiffrement.
Dès lors que l'on pose les questions suivantes, la réponse est souvent non : est-ce que les utilisateurs ont la maitrise du chiffrement ? Est-ce que les entreprises, en particulier PME, savent gérer leur implémentation ? Faut-il chiffrer son PC ?...

✓ Sensibiliser au chiffrement

Il s'agit d'encourager l'adoption d'un chiffrement généralisé et d'expliquer en quoi il est nécessaire.

❖ Sensibiliser les pouvoirs publics aux problématiques du secteur

Il est certain que les données sont maintenant de plus en plus présentes : plus d'utilisateurs, plus d'échanges, plus d'infrastructures numériques, plus d'objets connectés en circulation. Les menaces sont, corrélativement, en augmentation continue : atteinte aux données, collecte illicite de données confidentielles, accès non autorisé à des données sensibles, vol d'identité, perte ou destruction de données par exemple.
Dans de telles circonstances, le chiffrement joue un rôle de protection. Les pouvoirs publics doivent donc comprendre cette technique et saisir toute opportunité de dialogue avec les entreprises du secteur.

❖ Les entreprises doivent investir dans le chiffrement

Une entreprise sensibilisée à l'importance du chiffrement doit y consacrer un budget. Sous-investir en matière de sécurité est une mauvaise pratique car la sécurité sera faible et expose les actifs de l'entreprise à une attaque. En outre, combattre une attaque est bien plus coûteux que de sécuriser les actifs de l'entreprise en amont.

Pour cela, il est nécessaire que l'entreprise identifie les risques et failles à protéger.

D'après le CNNum : « *Pour les entreprises, le chiffrement est aujourd'hui le meilleur rempart contre l'espionnage économique qui a fait perdre plus de 40 milliards d'euros aux entreprises françaises en 2013. Les PME sont les premières victimes de ces cyberattaques car elles n'ont généralement pas les moyens d'un chiffrement robuste* » [11].

[11] Tribune « chiffrement et lutte contre le terrorisme : attention à ne pas se tromper de cible », publiée dans le Monde du 22 août 2016.

❖ Les entreprises du secteur de la cybersécurité doivent investir dans la R&D

Les entreprises doivent également investir dans la R&D liée au chiffrement. Il s'agit de maintenir la protection à jour et d'anticiper les nouvelles techniques qui offrent de nouvelles possibilités d'attaques à des personnes malveillantes.

❖ Sensibiliser à la gestion des clés

Les entreprises, en particulier les PME, doivent gérer les clés de chiffrement de leurs données. A défaut, elles seront leurs propres victimes, soit de se faire dérober ses clés, soit de les "perdre" et ainsi ne pas pouvoir relire des archives stockées sur des supports matériels. Les usages du cloud pour le stockage ne font que renforcer ce besoin de sensibilisation car *in fine,* c'est l'entreprise qui est responsable de ses données.

✓ Assurer un haut niveau de confiance

Les entreprises, fournisseurs de solutions, doivent créer des produits ergonomiques, faciles à utiliser et transparents. En faisant cela, si les produits sont neutres, non intrusifs, ils seront utilisés par les utilisateurs. De plus, par ces produits fiables et simples d'utilisation elles maintiennent la confiance des entreprises, de l'Etat et des consommateurs. Or, c'est la confiance qui permet la continuité des échanges et la stabilité de l'économie.

Cela nécessite que :

- Les prestataires de cybersécurité innovent en permanence, modernisent leurs produits et assurent les mises à jour régulières.
- Les entreprises développent des produits protégés, notamment dans le domaine du Cloud et des objets connectés.

- Les pouvoirs publics doivent :

✓ Promouvoir le chiffrement

Dans son rôle régalien, l'Etat doit prendre en considération les bénéfices du chiffrement en matière économique (protection des entreprises, des secrets d'affaires …), des citoyens (conservation de leurs données de santé en ligne de photos dans le Cloud, moins de risques d'interception des conversations …), en matière de sécurité (conserver la confidentialité des données contre des attaques sophistiquées).

✓ Mieux utiliser le chiffrement

Au lieu de chercher à affaiblir la cryptographie ou à introduire des portes dérobées dans les technologies, les autorités devraient chercher à rendre plus difficiles les actions des criminels : en se dotant d'outils d'investigation performant, en renforçant les mécanismes de partenariats et de coopération internationale, en se dotant d'outils d'investigation en temps réels (améliorer la coopération secteur privé / public ; renforcement de la coopération judiciaire dans l'UE et au-delà).

Le chiffrement est une nécessité absolue dans la confiance accordée aux moyens numériques par les citoyens, les entreprises et les gouvernements. Tout doit être fait pour ne pas en compromettre l'usage et la qualité des produits. La confiance réside aussi dans la capacité des gouvernements à assurer les fonctions régaliennes de Justice et de Défense. L'équilibre ne peut passer que par un dialogue clair entre les acteurs du secteur privé et public, arbitré par les citoyens.

Il est enfin inutile de légiférer à nouveau sur le chiffrement. Les services de sécurité doivent mieux exploiter les ouvertures légales qui leur ont été données par le législateur.

✓ Harmoniser les réglementations

Les Etats doivent harmoniser au niveau européen et international les règlementations encadrant le chiffrement, en revendiquant le plus haut niveau de sécurité possible.
Le comité cybersécurité encourage les Etats à développer des mécanismes de partenariats et de coopérations internationales, à améliorer la coopération secteur privé / public et à renforcer la coopération judiciaire dans l'UE et au-delà.

En France, le toilettage de la loi pour la confiance dans l'économie numérique s'avère nécessaire afin de la mettre à jour.

✓ Renforcer le dialogue entre l'ANSSI, les autorités et les prestataires en cybersécurité

En France, l'Agence Nationale de la Sécurité des Systèmes d'Information (« ANSSI ») doit partager des bonnes pratiques et sa feuille de route afin que les prestataires en cybersécurité soient informés et commercialisent des produits conformes et efficaces.

Un dialogue entreprises / pouvoirs publics peut être rapidement mis en place. Les syndicats professionnels peuvent réunir des entreprises qui serviront de « bêta-testeurs » des solutions proposées ou feront des propositions.

L'amélioration du dialogue entreprises / autorités de police ou judiciaire peut être mis en place.
Le CNNUm dans sa tribune évoque la coopération avec les fournisseurs de produits et de services sécurisés dans l'accès judiciaire aux données. Il s'agit de l'une des procédures à privilégier : « *Il serait en effet opportun de travailler à renforcer les règles de coopération judiciaire, en particulier les mutual legal assistance treaty (MLAT) – accords bilatéraux entre États qui permettent l'échange d'informations et de données lors d'enquêtes en cours – afin de réduire ces délais de transmission. C'est ce qui devrait être le sens d'une initiative internationale* ».

✓ Permettre la continuité de la circulation des données dans le marché unique numérique

Cette continuité passe par la protection des infrastructures et leur adaptation aux évolutions numériques. Le marché unique ne pourra être mis en place que par une reconnaissance de l'importance du chiffrement et son harmonisation au plan européen. Toute initiative qui entravera la mise en place de mesures de sécurité de l'information, à une échelle française et européenne, sera contreproductive.

✓ Assurer un cadre favorable à l'importation, l'utilisation et la vente de produits de chiffrement ou cryptographiques

✓ Assurer un fonds européen de dotation permettant de financer la R&D liée au chiffrement et la cryptologie

Le fonds servirait de relais entre les entreprises et les pouvoirs publics, entre les anciennes techniques et les nouvelles techniques (ex. blockchain).

- **Les citoyens doivent :**

Principalement se former au numérique et au chiffrement.

A terme, ils doivent mesurer l'impact de sécurité ou d'intégrité des données (quelles données sont chiffrées ou en clair, pour combien de temps), comprendre l'utilité de sécurisation des données dans leur vie numérique.