



Les objets connectés chez les moins de 6 ans

Travaux complémentaires- Février 2019



M2 - Marques et Produits Jeunesse
Dans le cadre du cours de Christian Gautellier
Andrea Arosteguy - Narimane Ayad - Florine Bouchet - Nardine
Marzouk



Sommaire

	Introduction	p.2
I.	Les objets connectés entre solutions et enjeux	p.3-8
	A) Copain ? Le livre à réalité augmentée signé Charlotte Gastaut - Edition Albin Michel p.3	
	B) Thermomètre portable Fever Scout.....	p.4-6
	C) iBaby Care M7 - le moniteur intelligent de surveillance pour bébé p.6-7	
	D) La brosse à dents intelligente Kolibree.....	p.7-8
II.	Les objets connectés et leurs multiples polémiques..	p. 9-17
	A) Le robot intelligent i-Que : une menace ?	p.10-11
	B) Les CloudPets : des vulnérabilités importantes.....	p.11
	B.1. 2017 : failles dans le système d'exploitation des données.....	p.11
	B.2. 2018 : failles dans le système de sécurité et suppression des ventes	p.12
	C) Le furby connecté : Hasbro se défend.....	p.13-15
	D) Le Toy-Fi Teddy soit le « champion de la négligence sécuritaire » p.15-17	
III.	Sur le plan national : la loi Informatique et Libertés. p.17-21	
	A) Le rôle de la CNIL.....	p.18
	B) Le principe de loyauté.....	p.19
	C) Les sanctions relatives au non-respect de la loi.....	p.19
	D) Au niveau européen : Le RGPD.....	p.19
	D.1 Les principes de « Privacy by design and default ».....	p.29
	D.2. Le droit à l'oubli numérique et la majorité numérique.....	p.20
	D.3. Les sanctions relatives au non-respect du règlement.....	p.20
	E) L'exemple de la Californie à l'international.....	p.21
IV.	Les Normes : un cadre qui évolue.....	p. 21-26
	A) Normes liées à l'aspect physique.....	p.21
	B) Normes liées à la sécurité des jouets électriques.....	p. 22-24
V.	Des petits conseils pour parents.....	p.25
	Conclusion.....	p. 27

Introduction

Estimé à plus de 15 milliards d'unités dans le monde en 2015, les objets connectés ou les Internet of Things (IoT) s'associent peu à peu à notre vie quotidienne à travers une ergonomie de plus en plus imperceptible, ciblant toutes les générations, y compris les plus jeunes.¹

Dans de précédents travaux relatifs à ce nouveau phénomène, et dans leur article intitulé « Analyse de l'offre numérique destinée aux jeunes enfants de 0 à 6 ans », Valérie-Inés de LA VILLE et Tatiana PICQ ont réussi, à partir de 83 produits et services numériques étudiés à destination des enfants de moins de six ans, à définir quatre classes² d'objets connectés répondant à des enjeux similaires sur le plan du développement de l'enfant et de l'accompagnement du parent dans l'exercice de sa responsabilité parentale.

Ces dernières s'inscrivent dans des promesses allant de la surveillance de l'enfant à son divertissement, en passant par un développement précoce de ses capacités sociales et intellectuelles, ainsi que l'assurance de son autonomie.

Par ailleurs, les arguments marketing qui défendent ces objets, s'appuient fortement sur le caractère « Peace Of Mind » qu'ils peuvent apporter aux parents en réponse à la dimension anxiogène qui les caractérise.

Cela dit, il va sans dire que nombre de ces objets connectés, cachent derrière leur discours mielleux, une réalité obscure qui se nourrit d'une éthique à contester fortement.

Dans ce présent document, nous allons essayer de faire suite aux travaux de Valérie-Inés de LA VILLE et Tatiana PICQ, à travers, en premier lieu, une remise en question des pratiques qu'emploient les objets connectés qui, à priori, semblent bénéfiques à bien des égards aussi bien pour l'enfant que pour les parents, tout en proposant des recommandations permettant de réduire les risques que nous pouvons encourir en les utilisant.

En deuxième lieu, nous marquerons une halte devant les objets connectés qui ont fait polémique, et qui ont même fait l'objet d'un retrait du marché, tant ils représentent un danger pour l'enfant et sa famille.

1 <http://www.marketing-professionnel.fr/parole-expert/objets-connectes-internet-des-objets-iot-enfants-201504.html>

2 Quantified kids, Préparation à l'école, Exhausteurs de créativité et d'imagination, Activités du quotidien

Document de travail. Cepe, IAE Poitiers et Ceméa. Mai 2019

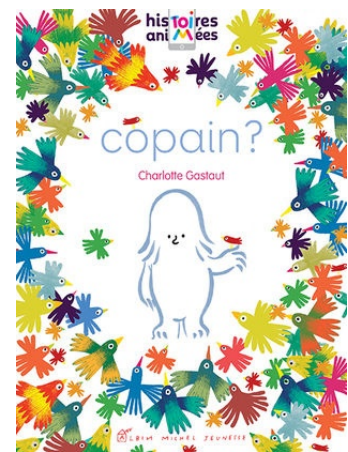
Enfin, nous mettrons en lumière les normes et textes juridiques qui tentent de cadrer et de réglementer ce nouveau secteur, de plus en plus présent dans notre vie quotidienne.

I. Les objets connectés entre solutions et enjeux

Dans leur communication, les objets connectés se veulent utiles et rassurants pour les parents, ludiques et éducatifs pour les enfants.

Ci-après, nous citerons des exemples véhiculant ces valeurs, et relèverons la question d'éthique qui les caractérise.

A. Copain ? Le livre à réalité augmentée signé Charlotte Gastaut - Edition Albin Michel



Destiné aux enfants de trois ans et plus, « Copain ? » est un livre illustré, connecté à une application **gratuite** sur Android ou Apple, permettant à ses jeunes utilisateurs de visualiser, à travers un smartphone ou une tablette, une collection d'albums illustrés qui prend vie, où *le rien devient quelqu'un, le vide devient plein, l'attente devient partage, et par une habile pirouette finale, imaginaire et réel se mêlent avec poésie*.³

Via ces illustrations, l'enfant vit une expérience narrative hybride, où papier et numérique s'allient pour lui faire découvrir une nouvelle façon d'appréhender les livres. En effet, les livres aujourd'hui, s'inscrivent à leur tour dans la réalité augmentée. Chose qui permet aux lecteurs (notamment les enfants), d'approcher un contenu enrichi, de stimuler leur imagination, et de renforcer leur engagement et motivation à l'égard de l'apprentissage⁴.

Par ailleurs, la réalité augmentée permet un enseignement qui va au-delà de la platitude des images qu'offre un livre illustré ordinaire. Elle invite le lecteur à acquérir une force de visualisation d'un environnement en 3D plus réaliste sous tous les aspects possibles, conforte son acquisition du savoir, et le familiarise en douceur avec les nouvelles technologies.⁵

³ <https://www.albin-michel.fr/ouvrages/copain-9782226325150>

⁴ <https://fr.yeepley.com/blog/realite-augmentee-education/>

⁵ Ibid

Afin de pouvoir bénéficier de pareille expérience, il est nécessaire de se connecter sur une application.

Dans le cas de « Copain ? », nous avons tenté de le faire. Toutefois, lors des étapes de l'installation, l'accès aux fichiers multimédia, images, vidéos et caméra est requis pour pouvoir mener à bien l'opération. Chose qui nous amène à questionner le caractère gratuit de l'application ; Si le livre est à hauteur de 15 €, la gratuité de l'application représente la contrepartie de notre cession de données personnelles susceptibles d'être rachetées par des organismes tierces, ou utilisées à des fins que nous ignorons.

Ainsi, nous pouvons croire que ceci s'inscrit dans une dimension où l'on est contraint d'accepter un service contre un autre dont on ignore l'issue.

Se contenter d'un livre illustré en 2D sans prendre part au bénéfice qu'il propose semble une solution qui ne peut nous faire avancer.

Il serait nettement préférable si la construction du modèle économique du service offert change à travers :

- Une augmentation du prix du pack, en garantissant à l'utilisateur une totale transparence quant à l'accès à la caméra du device utilisé (car cet accès est réellement nécessaire pour pouvoir utiliser la réalité augmentée),
- Une demande de consentement de l'utilisateur vis-à-vis de l'exploitation de ses données personnelles (en précisant l'issue de leur utilisation) avec une possibilité de refus, sans que cela le contraigne à ne pas avoir accès au service
- L'agrémentation de l'offre du service avec des options payantes (tel qu'une customisation du personnage,...) permettant à l'utilisateur d'accepter ou non de se les procurer, sans que cela l'oblige à abandonner le bénéfice initial de l'offre.



Ainsi, utilisateur et prestataire de l'offre trouvent leur compte !

B. Thermomètre portable Fever Scout

A la forme d'un patch souple, flexible et difficilement détectable, Fever Scout est un thermomètre portable dotée d'une application permettant la collecte de la température de l'enfant toutes les minutes, envoie les données collectées à une application mobile installée sur l'appareil des parents sous forme de graphiques leur permettant de visualiser une image claire de la température de leur enfant.⁶

Il permet une surveillance automatisée (avec réception d'alertes dès que la fièvre augmente), où que la parent soit (dans une autre chambre ou

⁶ <https://meee-services.com/what-are-the-best-iot-based-children-safety-devices/>

dans une autre ville), et un partage d'informations faciles avec le médecin via la documentation de symptômes et médicaments à travers l'application.⁷

Ce thermomètre, conçu par l'entreprise VivaLNK, fournisseur de solutions médicales connectées, relève l'approbation de nombreux parents. La

★★★★★

Adam le 17 avr. 2017

Ce produit est incroyable !!

Ce produit est absolument incroyable. Mon fils a des crises fébriles et je pense que cela aidera beaucoup! cela m'aidera à dormir un peu quand mon LO sera fébrile. Mon fils fait des crises fébriles, ce qui nous permet de suivre ses températures. Je ne peux pas exagérer à quel point je suis impressionné par ce produit. Je suis tellement excité! Ce serait le cadeau de naissance idéal ou n'importe quel cadeau! Je me sens plus confiant dans les soins que je peux fournir à mon enfant malade avec l'aide de ce produit. Je n'ai pas été payé pour écrire une critique, j'ai reçu le produit gratuitement. Il a dépassé toutes mes attentes et plus encore. C'est une nécessité absolue pour quiconque a des enfants qui souffrent de crises fébriles. Je recherche ce type de produit depuis si longtemps maintenant ... et je suis si heureux d'en avoir enfin un! Je suis une maman excitée!

plupart adhère à l'utilisation de ce patch au cas où leurs enfants sont

★★★★★

Marcie F. le 16 février 2018

Jusqu'ici tout va bien

Nous ne l'avons utilisé qu'une fois jusqu'à présent. Notre petite fille avait une faible fièvre, mais habituellement, quand elle est malade, elle se réchauffe rapidement et toute la nuit. Je pouvais suivre sa température toute la nuit sans la réveiller du tout. J'aime cela!! Garde mon esprit inquiet de maman à l'aise!

atteints de fièvre ; les commentaires sur le site Internet du produit <https://feverscout.com/products/fever-scout#technicalspecs> y attestent.

Dans la mesure où cet objet connecté se place au niveau de l'aisselle de l'enfant, nous nous sommes toutefois posé la question quant au danger des ondes de cet appareil sur la santé de son utilisateur. Nous nous sommes donc penchés sur ses caractéristiques, et nous sommes allés chercher s'il était conforme aux normes de sécurité sanitaire.

Dans nos recherches, nous avons trouvé que Fever Scout utilise la technologie BLE (Bluetooth Low Energy), dont le ratio spécifique d'absorption est de 0.0001 watts/kg, soit moins d'un millième de la norme établi par la FDA (US Food and Drugs Administration) pour les téléphones cellulaires. Par ailleurs, le Bluetooth émet moins d'ondes que les smartphones ou les appareils utilisant la Wi-Fi.

Bien que cela soit vrai, les spécialistes mettent en garde de mettre des objets connectés au contact du corps car ils permettent une exposition des parties du corps à proximité immédiate à des émissions parfois permanentes tant que l'objet est allumé. Ils conseillent par la même occasion d'éviter que les bébés et les enfants de s'y exposer.⁸

⁷ <https://meee-services.com/what-are-the-best-iot-based-children-safety-devices/>

⁸ <https://www.lesoir.be/art/1479461/article/soirmag/soir-mag-sante/2017-04-10/bluetooth-risque-mais-pas-trop>

A ce titre, nous avons examiné si les concepteurs de Fever Scout étaient conscients de ce danger. Il s'est avéré que ce produit est approuvé par la FDA (US Food and Drugs Administration), et qu'un corps médical est derrière pour apporter des conseils à l'entreprise VivaLNK. Aucun n'a remis en cause l'utilité de ce produit, ni même ses potentiels dangers. Aussi, l'OMS a déclaré qu'après plusieurs années d'études et malgré de nombreuses recherches, rien n'indique pour l'instant que l'exposition à des champs électromagnétiques de faible intensité soit dangereuse pour la santé humaine ».

Pour ce faire, doit-on nous conformer à ce genre de dispositif pour se procurer un semblant de « Peace of Mind », en attendant une nouvelle étude qui déconseillerait son utilisation, ou doit-on prendre les devants en prévenant tout risque susceptible d'atteindre la santé de nos enfants ?

De plus, est-ce réellement un objet nécessaire, en dépit de l'adhésion de tous à s'accorder que Fever Scout est le remède miracle à tous les maux fiévreux ?

Vraisemblablement, non. Ce patch connecté pourrait très bien être remplacé par une surveillance parentale aussi efficace qu'elle l'a été il y a encore moins de cinq ans.



C. iBaby Care M7 - le moniteur intelligent de surveillance pour bébé

Doté d'une résolution vidéo 1080p Siphon Moonlight intégré, d'un support de routeur double bande, d'un capteur de qualité de l'air 2.4Ghz et 5Ghz COVT, d'alertes "couche et d'alimentation", de projections au clair de lune et d'un contenu éducatif précoce, iBaby Care M7 est un moniteur connecté au smartphone des parents via une application, à travers laquelle ils peuvent visionner leur enfant et s'assurer qu'il ne manque de rien.⁹

A la promesse habituelle de "Peace Of Mind", cet objet connecté certifié FCC CE ROHS RCM KC, est titulaire de nombre de prix, tels que le Tillywig award winner (Parent's favorite products), 2018 national parenting product awards et le Mom's choice awards (Honoring Excellence). Toutefois, aucune mention n'a été faite par les associations de consommateurs américaines.

De plus, ce produit est un objet qui collecte les données personnelles des parents et enfants, sauf qu'à l'opposé de nombreux concurrents, sa politique concernant cet angle est claire.

Sur son site Internet <https://ibabylabs.com/privacy-policy/>, il explique clairement à ses utilisateurs qu'il ne vend, ni loue ces données personnelles, et les utilise à des fins statistiques de manière anonymes.

⁹ <https://ibabylabs.com/>

Personal identification information

We may collect personal identification information from Users in a variety of ways, including, but not limited to, when Users visit our site or Apps, register on the site or Apps, place an order, subscribe to the newsletter, respond to a survey, fill out a form, and in connection with other activities, services, features or resources we make available on our Site or Apps. Users may be asked for, as appropriate, name, email address, mailing address, phone number. Users may, however, visit our Site or Apps anonymously. We will collect personal identification information from Users only if they voluntarily submit such information to us. Users can always refuse to supply personally identification information, except that it may prevent them from engaging in certain Site or Apps related activities.

Sharing your personal information

We do not sell, trade, or rent Users personal identification information to others. We may share generic aggregated demographic information not linked to any personal identification information regarding visitors and users with our business partners, trusted affiliates and advertisers for the purposes outlined above.

Compliance with children's online privacy protection act

Protecting the privacy of the very young is especially important. For that reason, we never collect or maintain information at our Site or Apps from those we actually know are under 13, and no part of our website or Apps is structured to attract anyone under 13.

Aussi, concernant les ondes électromagnétiques, il est important de noter qu'en dépit du fait qu'aucune preuve attestant qu'elles puissent constituer un danger sur la santé des bébés, il serait préférable d'éviter ce genre d'équipement tant ces jeunes enfants représentent une population sensible, et sont les premiers à être exposés à ce genre d'ondes avant même leur naissance. Chose qui nous amène à croire que la science a été dépassée par les avancées technologiques, et n'a donc pas assez de recul pour émettre des conclusions claires et incontestables à ce sujet.

Par ailleurs, les arguments marketing de ce produit aux multiples prix, demeurent toutefois reposés sur le caractère anxiogène que ces adultes avec enfants adoptent, ce qui remet en cause sa dimension éthique.

Enfin, de même que l'ensemble des objets connectés commercialisés aujourd'hui, iBaby Care M7 renforce cette relation familiale dématérialisée, que nous craignons, fasse partie intégrante de notre vie quotidienne très prochainement...

D. La brosse à dents intelligente Kolibree

Aux poils ronds, évitant ainsi aux enfants de se gratter les gencives lorsqu'ils se brossent les dents, Kolibree est une brosse à dent qui élimine les plaques grâce à son action sonique. Connectée à une application mobile, elle permet d'enseigner à l'enfant les bonnes habitudes dentaires, tout en le surveillant à l'action du brossage de dents, pour les envoyer aux parents, leur épargnant pour l'occasion, de le contrôler en permanence.¹⁰

Grâce à une connexion Bluetooth, qui transforme la brosse à dents en une manette de jeu, les enfants s'amuse tout en se brossant les dents.

Les jeux ont été conçus pour qu'ils brossent bien toutes les dents pendant deux minutes, le temps recommandé par les dentistes.¹¹

Cependant, comme tout objet connecté, ce produit collecte les données personnelles de ses utilisateurs. Il déclare sur son site qu'il ne les vend



¹⁰ <https://meee-services.com/what-are-the-best-iot-based-children-safety-devices/>

¹¹ <https://www.kolibree.com/fr/families/>

pas ni les loue, mais il s'en sert à des fins promotionnelles en implantant des cookies sur leur ordinateur.¹²

Chose qui nous amène à réfléchir quant aux contreparties requises incessamment pour apporter une solution à laquelle nous ne sommes pas contraints d'y adhérer.

Sommes-nous finalement réduits à faire face à cette stratégie contre notre propre volatilité ou devrions-nous nous soumettre à cette nouvelle tendance qui promet de s'incruster dans les moindres pans de notre quotidien ?

Les exemples que nous venons de citer sont tous à prime à bord utiles pour l'enfant et/ou les parents. Toutefois, en plus de leur connotation anxiogène remettant en cause leur dimension éthique, ils constituent les uns et les autres, un potentiel danger pour la santé et la vie privée de l'enfant et de sa famille : allant de la collecte de données personnelles à l'émission d'ondes électromagnétiques, en passant par une dématérialisation des relations familiales, leur utilité dans notre vie quotidienne devient contestable.

Néanmoins, des compromis sont possibles lorsqu'il n'est pas question de la santé de son enfant. Un modèle économique susceptible de convenir aussi bien aux parents qu'aux industriels est envisageable, et la transparence quant à l'utilisation des données personnelles est concevable.

Dans deuxième partie de ce document, un autre genre d'objets connectés sera étudié. Il s'agit de ceux qui ont fait polémique, tant leur commercialisation constitue un réel danger pour la vie privée des familles, notamment celles des enfants.

A ce titre, après l'analyse d'un contexte plutôt positif en ce qui concerne les objets connectés, il ne faut pas oublier qu'une réalité tout autre se dessine, encore méconnue par le grand public et également, par les professionnels. Malgré un horizon positif (environ 30 objets connectés d'ici 2020)¹³, beaucoup de polémiques sont soulevées sur la fiabilité, l'utilisation de données personnelles et la sécurité de ces objets. En effet, tous les objets connectés ne sont pas fiables ni sécurisés et ont même été retirés de la vente pour captation illégales de données, tracking et piratage. Après la suppression des ventes de la poupée « Cayla » en 2017, peut-on réellement avoir confiance en eux ? Les enfants sont-ils vraiment en sécurité ? Quels sont les dangers ? Nous allons essayer de comprendre et d'analyser les divers enjeux que nous imposent ces objets connectés de plus en plus nombreux sur le marché et les risques pour les enfants.

12 https://www.kolibree.com/fr/privacy_policy/

13 Maddyne : <https://www.maddyne.com/2018/08/17/iot-objets-connectes-inutile/>
Document de travail. Cepe, IAE Poitiers et Ceméa. Mai 2019

II. Les objets connectés et leurs multiples polémiques

Les jouets dits « intelligents » sont aujourd'hui incontournables. Originales et séducteurs ces jouets ont tout pour plaire, mais c'est sans compter sur les pirates qui profitent des vulnérabilités de ces jouets pour pouvoir les exploiter et entrer dans l'intimité des foyers.

Pourquoi sont-ils si vulnérables ?

- Les fabricants ne font pas assez attention à la sécurité lorsqu'ils fabriquent leurs jouets. Cela est sûrement dû à un manque d'expertise de la part de ces professionnels comme c'est le cas dans beaucoup de secteurs et pas uniquement les jeux et jouets (exemple : Motorola qui fabrique des babyphones connectés).
- Ce manque d'expertise de la part des fabricants est également présent chez les consommateurs qui sont encore loin d'imaginer ce que peut provoquer le piratage d'un jouet connecté. Attirés par la nouveauté et les nouvelles fonctionnalités, la sécurité leur importe peu.
- Une réglementation quasi-inexistante ; « il n'existe toujours aucune norme, ni contrôle de sécurité pour 90% des appareils disponibles sur le marché »¹⁴

Pour pallier cela, diverses choses sont donc mises en place pour éveiller et responsabiliser la population (professionnels et particuliers) sur ces nouveaux objets, comme cette vidéo qui démontre qu'il est de plus en plus facile de pirater les jouets connectés pour enfants : <https://www.youtube.com/watch?v=Ogy7xjEWEpo>

Également, une infographie réalisée par la CNIL a été mise en ligne pour aider les individus à comprendre comment un ours en peluche connecté peut être piraté s'il est mal sécurisé et des conseils pour éviter que cela se produise.¹⁵

A partir de 2017, l'association allemande « Stiftung Warentest » (l'équivalent d'UFC Que-Choisir), l'association britannique experte en sécurité « Which ? » et divers cabinets d'études spécialisés en sécurité ont fait plusieurs expériences pour déterminer les failles de sécurités. Résultats : sur 7 produits connectés, 4 présentent d'importantes vulnérabilités. Ces jouets sont assez populaires et ont une bonne position dans les ventes de jouets. Il s'agit du :

¹⁴ Programmez : <https://www.programmez.com/avis-experts/le-jouet-intelligent-le-cadeau-de-noel-ideal-pour-les-pirates-28363>

¹⁵ CNIL : <https://www.cnil.fr/fr/infographie-il-etait-une-fois-lours-connecte-mal-securise>

- ⇒ Furby Connect
- ⇒ CloudPets
- ⇒ Robot i-Que
- ⇒ Toy-fi Teddy

Les résultats de ces jouets ont révélé plusieurs failles dans les dispositifs de sécurité avec une connexion Bluetooth non sécurisée (pas d'authentification, ni de mots de passe) ce qui veut dire que n'importe qui peut s'y connecter et prendre la possession du jouet à 10 mètres avec possibilité d'étendre la connexion Bluetooth.



Il est important de noter que le robot i-Que et Toy-Fi Teddy avaient déjà été répertoriés comme les jouets les plus faciles à pirater selon UFC Que Choisir¹⁶. Également, ces quatre mêmes jouets, ont retenu l'attention de « Which ? », une association de consommateurs britanniques, qui

souhaite les retirer de la vente.¹⁷

A. Le robot intelligent i-Que : une menace ?

Le robot i-Que, fabriqué par « Genesis Toys », communique avec les enfants via un système de micros et d'un haut-parleur, reliés à Internet par une application mobile.

- **En 2017**, en plus de l'enquête qu'a été faite par les experts en sécurité, la CNIL a elle aussi voulu vérifier la fiabilité de la sécurité et est arrivée au même résultat, le robot i-Que avait un défaut de sécurité. Dans un communiqué elle déclare :

« Une personne située à 9 mètres des jouets à l'extérieur d'un bâtiment peut connecter un téléphone mobile aux jouets grâce au standard de communication Bluetooth sans avoir à s'authentifier. » De plus, « la personne située à une telle distance est en mesure d'entendre et d'enregistrer les paroles échangées entre l'enfant et le jouet ou encore toute conversation se déroulant à proximité de celui-ci »¹⁸

L'association allemande de consommateurs « Stiftung Warentest » a passé des tests sur ce robot. Résultat : le piratage n'a pas été difficile ce qui a agrandi leurs inquiétudes ;

« Cette faille de sécurité est extrêmement critique, toute personne qui possède un smartphone peut contrôler le robot, l'utiliser comme

¹⁶ UFC Que Choisir : <https://www.quechoisir.org/actualite-jouets-connectes-trop-faciles-a-detourner-n46276/>

¹⁷ Numerama : <https://www.numerama.com/tech/305902-furby-robots-i-que-la-securite-de-certains-jouets-connectes-pose-toujours-probleme.html>

¹⁸ Le Monde : https://www.lemonde.fr/pixels/article/2017/12/04/jouets-connectes-la-cnil-met-en-demeure-le-fabricant-de-la-poupee-cayla-et-du-robot-i-que_5224291_4408996.html

mouchard, adresser des questions, des invitations, voire des menaces à l'enfant ! »¹⁹

Faillles relevées :

- Pas de sécurité au niveau de l'application

Conséquences :

- Tout le monde peut télécharger l'application et avoir accès au robot i-Que connecté autour de soi en Bluetooth sans besoin de mots de passe
- Prise du contrôle du robot, « lui faire dire ce qu'on transmet à l'écrit »²⁰ via un champ de texte
- Le robot a sa propre voix, ce qui veut dire que l'enfant peut lui faire confiance assez rapidement sans se soucier de qui est réellement connecté, et le pirate peut donc parler directement à l'enfant et écouter ses réponses
- Récupération de données personnelles

Retours des professionnels :

Ce signalement a directement été pris en compte par Vivi Toys, le distributeur britannique d'i-Que qui a déclaré : « *il n'a été signalé aucun cas d'utilisation malveillante de ces produits* »²¹ et qu'il allait informer le fabricant d'i-Que, Genesis Toys.



B. Les CloudPets : des vulnérabilités importantes

CloudPets est disponible sur Amazon et fabriqué par Spiral Toys. C'est un jouet rembourré qui permet à la famille et aux amis d'envoyer des messages vocaux à un enfant. Ces messages sont reproduits sur un haut-parleur intégré.

B.1. 2017 : failles dans le système d'exploitation des données

Victors Gevers, président de la « GDI Foundation » (association qui a pour objectif de rendre Internet plus sûr), a relevé qu'un lien Internet, en direction de la plateforme de stockage des informations (MongoDB), était mal protégé. Par conséquent, en une semaine, les données personnelles de 821 000 détenteurs de peluches CloudPets étaient accessibles, soit : ²²

- Les e-mails des comptes CloudPets et les mots de passe associés

19 UFC Que Choisir : <https://www.quechoisir.org/actualite-jouets-connectes-trop-faciles-a-detourner-n46276/>

20 Numerama : <https://www.numerama.com/tech/305902-furby-robots-i-que-la-securite-de-certains-jouets-connectes-pose-toujours-probleme.html>

21 Traduction du passage de l'article suivant : <https://www.which.co.uk/news/2017/11/safety-alert-see-how-easy-it-is-for-almost-anyone-to-hack-your-childs-connected-toys/>

22 Le Monde : https://www.lemonde.fr/pixels/article/2017/02/28/les-donnees-personnelles-de-800-000-propriteaires-d-ours-en-peluche-connectees-accessibles-sur-internet_5087012_4408996.html

- Les 2 millions de messages vocaux (avec parfois des demandes de rançons, preuves que des peluches ont été hackées peu après leur sortie)

Points de vue des professionnels :

- Troy Hunt, expert en sécurité web conseille les parents de retourner aux peluches plus traditionnelles à travers un discours :
« Les jouets qui enregistrent leur voix et envoient ces fichiers sur le Web posent de sérieux risques pour la vie privée. Ce n'est pas tant que ces risques soient différents de ceux auxquels vous faites face tous les jours avec le volume de données que vous produisez et mettez en ligne, mais plutôt que notre tolérance varie beaucoup lorsque des enfants sont impliqués. J'ai moi-même de jeunes enfants et, franchement, je ne vois pas l'utilité pour eux d'avoir des choses qui captent leurs voix et les stockent en ligne. »²³

B.2. 2018 : failles dans le système de sécurité et suppression des ventes

Expérience faite :

- Les experts en recherche ont réussi à pirater le système sur le CloudPets « chaton » et ont commandé de la nourriture pour chat auprès d'Amazon Echo.

Ils ont pu se connecter à la peluche interactive en étant à l'extérieur de la maison via le Bluetooth qui n'a demandé aucune identification.

Vous pouvez visualiser l'expérience sur ce lien : <https://www.which.co.uk/news/2017/11/safety-alert-see-how-easy-it-is-for-almost-anyone-to-hack-your-childs-connected-toys/>

Les failles relevées :

- Pirater le système et donc pouvoir faire ses propres messages vocaux ou, connecté à Alexa, pouvoir faire, au travers de la peluche, un achat sur Amazon Echo.
- Également, des chercheurs ont découvert que la plateforme où sont présents les utilisateurs « mycloudpets.com/tour », est un domaine actuellement en vente qui peut donc être possédé par de potentiels pirates. Il y a donc un risque de phishing.
- Les pirates auraient la possibilité d'installer un micrologiciel personnalisé sur le jouet sans aucune vérification de sécurité pour l'arrêter.

Retours des professionnels :

²³ Le Monde : https://www.lemonde.fr/pixels/article/2017/02/28/les-donnees-personnelles-de-800-000-propriteaires-d-ours-en-peluche-connectees-accessibles-sur-internet_5087012_4408996.html

- Spiral Toys n'a pas encore fait de retours concernant les failles de sécurités
- Depuis la relève de ses nombreuses failles, le fabricant n'a pas mis en place des techniques d'authentifications permettant de résoudre le problème²⁴

Nous pouvons donc noter trois grandes failles :

- Récupération de données personnelles à cause d'un lien défaillant
- Prendre le contrôle de la peluche via la plateforme d'application connectée à Bluetooth et qui ne nécessite pas d'authentification
- Vente d'un domaine de la plateforme ce qui est donc un risque pour un possible piratage

Les conséquences de ces piratages :

- Prendre le contrôle de la peluche et se connecter sur le compte, puis s'en servir pour envoyer n'importe quel contenu
- Possibilité de se connecter via le Bluetooth à une interface tierce pour enregistrer l'audio et envoyer des messages aux jouets
- Possibilité de transformer la peluche en mouchard qui est capable d'espionner les conversations et les envoyer vers n'importe quel serveur sous la forme de message de 40 secondes²⁵
- Récupération de données via la connexion Bluetooth et également, via le micrologiciel

Les risques de sécurité et de collectes illégales des données personnelles des utilisateurs de CloudPets étant trop importantes, les lobbyistes ont mis une pression pour que les ventes de ce produit cessent.

Ce fut aussi le cas pour la « Electronic Frontier Foundation » (association qui défend les libertés dans l'espace numérique) qui a demandé au travers d'une lettre adressée directement à Amazon de retirer ces produits de la vente.

Les professionnels aussi sont inquiets, comme nous pouvons le voir avec Ashley Boyd (vice-présidente de Mozilla) : « *Dans un monde où les fuites de données sont de plus en plus courantes et où des produits comme CloudPets restent sur les tablettes des magasins, je suis de plus en plus inquiète pour la confidentialité et la sécurité de mes enfants* »²⁶

Face à la pression et toute la polémique autour de ce produit, Amazon a donc décidé de retirer ces peluches des ventes.

²⁴ Electronic Frontier Foundation (EFF) - lettre d'association consommateurs : <https://www.eff.org/files/2018/05/28/cloudpetssignonletter.pdf>

²⁵ Generation-nt : <https://www.generation-nt.com/jouets-connectes-peluches-pirates-recuperation-800-000-comptes-donnees-personnelles-actualite-1940050.html>

²⁶ C net : <https://www.cnet.com/news/amazon-will-stop-selling-connected-toy-cloud-pets-filled-with-security-issues/>

C. Le furby connecté : Hasbro se défend

Les failles :

- Le furby connect de chez Hasbro, peut être piraté de la même manière que le robot i-Que : toute personne accédant à Bluetooth peut y voir le jouet et s'y connecter. Car, tout comme le robot, il n'y a aucune page d'authentification pour pouvoir se connecter. Globalement, cette faille permet à toute personne « présente dans un périmètre de 10 à 30 mètres de se connecter au jouet sans fournir de mot de passe ou le moindre type d'identification ». ²⁷

Voici sur ce lien une vidéo qui illustre les travaux de Florian Euchner (expert en sécurité), pour prouver que lorsqu'un Furby est piraté il est possible d'envoyer n'importe quel fichier audio. Également, comme il est possible de transformer le Furby en « périphérique d'écoute »²⁸ : https://www.youtube.com/watch?v=FkblA_CxHgU.

Les conséquences :

- Contrôle de la peluche connectée et envoi de fichiers non adaptés pour des enfants
- Possibilité d'entreprendre des conversations avec les enfants
- Possibilité d'écoute et d'enregistrement illégal (espionnage)
- Récupération des données personnelles

Le retour des fabricants :

Pour Hasbro, ces vulnérabilités ne pourraient se présenter que si la personne qui souhaite s'introduire dans le système soit experte et qu'elle possède les connaissances techniques nécessaires : « *Nous sommes convaincus que la conception de notre produit et de son appli garantissent sa sécurité. Le Furby Connect [...] n'a pas été conçu pour récolter le nom, l'adresse ou les informations de contact en ligne des utilisateurs. [...] [Le jouet] ne recourt pas au microphone de votre appareil et n'enregistre pas votre voix.* »²⁹

Le point de vente Argos souligne : « *La sécurité des produits que nous vendons est extrêmement importante pour nous. Nous n'avons reçu aucune plainte concernant ces produits, mais nous sommes en contact étroit avec les fabricants, qui étudient déjà ces recommandations* »³⁰



²⁷ Numerama : <https://www.numerama.com/tech/305902-furby-robots-i-que-la-securite-de-certains-jouets-connectes-pose-toujours-probleme.html>

²⁸ Which ? : <https://www.which.co.uk/news/2017/11/safety-alert-see-how-easy-it-is-for-almost-anyone-to-hack-your-childs-connected-toys/>

²⁹ Numerama : <https://www.numerama.com/tech/305902-furby-robots-i-que-la-securite-de-certains-jouets-connectes-pose-toujours-probleme.html>

De plus, « La British Toy and Hobby Association » dont Vivid le distributeur et Hasbro sont membres déclarent : « *Le secteur assume incroyablement ses responsabilités lorsqu'il fabrique des produits pour enfants. Les membres de BTHA investissent énormément dans la sécurité des jouets, la confidentialité des données et la sécurité en ligne. Nous sommes au courant du dossier de Which ?, mais comprendre les circonstances dans lesquelles ces enquêtes ont eu lieu reposent sur un ensemble parfait de circonstances et la manipulation des jouets et du logiciel qui rend le résultat très improbable dans la réalité* »³¹



Mais les doutes persistent et s'accumulent, comme c'est le cas pour Alex Neill (responsable des produits et services de maison de « Which ? » qui souligne auprès du magazine « The Guardian »³² : « *Les jouets connectés sont de plus en plus populaires, mais, comme le montre notre enquête, les clients qui envisagent d'en acheter devraient se montrer prudents. La sécurité est la priorité de tout type de jouet. Si elle ne peut être garantie, les produits ne devraient pas être vendus* » Which ? demande leur suppression de ventes.

Une association de consommateur a d'ailleurs aussi demandé la suppression des ventes de ces produits aux États-Unis.

D. Le Toy-Fi Teddy soit le « champion de la négligence sécuritaire »³³

Le Toy-Fi Teddy disponible sur Amazon et fabriqué par Spiral Toys (même fabricant que le CloudsPets) est un petit nounours avec un cœur rouge sur la poitrine qui permet à l'enfant d'envoyer et de recevoir des messages personnels enregistrés sur une plateforme via Bluetooth.

Les failles :

- Une enquête est menée par « Stiftung Warentest » (l'équivalent allemand de « Que Choisir »), qui a constaté comme la plupart des experts, qu'il était facile de se connecter à la peluche via le Bluetooth qui ne nécessite aucune authentification.
- Possibilité de mettre des traceurs
- Faille dans la régulation des données personnelles

Les conséquences :

30 The Guardian (discours traduit) : <https://www.theguardian.com/technology/2017/nov/14/retailers-urged-to-withdraw-toys-that-allow-hackers-to-talk-to-children>

31 The Gardian (texte traduit) : <https://www.theguardian.com/technology/2017/nov/14/retailers-urged-to-withdraw-toys-that-allow-hackers-to-talk-to-children>

32 The Guardian : <https://www.theguardian.com/technology/2017/nov/14/retailers-urged-to-withdraw-toys-that-allow-hackers-to-talk-to-children>

33 Motherboard : <https://motherboard.vice.com/fr/article/evb77j/pour-noel-offrez-des-jouets-connectes-vulnerables-a-vos-gamins>

- Des étrangers peuvent prendre le contrôle de la peluche et envoyer des messages vocaux aux enfants, recevoir la réponse des enfants sur une distance de 10 à 30 mètres avec possibilité d'avoir une antenne bricolée chez soi pour augmenter la portée du signal
- Traceurs : possibilité de reconstituer les déplacements³⁴
- Il y a eu, à cause de la faille des données personnelles, certaines données qui ont été envoyées à Google ou à des tiers à des fins publicitaires

Le retour des fabricants :

- Tout comme la polémique avec CloudsPets, le fabricant n'a pas donné de retour sur cette étude.

Après les polémiques, voici comment sont distribués ces jouets en France :

	Sites spécialisés	Sites e-commerces	GMS
Robot I-Que	Fnac : Oui Darty : Non Toys r us : Non King Jouet : Non La Grande Récré : Non Maxi Toys : Non	Amazon : Non Cdiscount : Non Ebay : Oui Rakuten : Oui Pixmania : Non	Auchan : Non Carrefour : Non Leclerc : Non
Clouds Pets	Fnac : Non Darty : Non Toys r us : Non King Jouet : Non La Grande Récré : Non Maxi Toys : Non	Amazon : Non, une offre, mais aucunes descriptions + impossible de cliquer sur le vendeur et pas d'avis donc offre non fiable et par conséquent pas notée + une autre offre mais les peluches ne sont pas connectées Cdiscount : Non Ebay : Non	Auchan : Non Carrefour : Non Leclerc : Non

³⁴ Midi Libre : <https://www.midilibre.fr/2017/12/05/vie-privee-alerte-sur-le-danger-des-jouets-connectes-avant-noel,1598354.php>

		Rakuten : Non Pixmania : Non	
Furby Connect	Fnac : Oui Darty : Oui Toys r us : Non King Jouet : Non La Grande Récré : Oui, mais pas les connectés Maxi Toys : Non	Amazon : Oui Cdiscount : Oui Ebay : Oui Rakuten : Oui (une seule offre par un particulier) Pixmania : Oui	Auchan : Non Carrefour : Non Leclerc : Non
Toy-Fi Teddy	Fnac : Non Darty : Non Toys r us : Non King Jouet : Non La Grande Récré : Non Maxi Toys : Non	Amazon : Oui mais une seule offre qui provient des USA à prix dérisoire pour une peluche connectée (26,36 euros) Cdiscount : Non Ebay : Oui, mais surtout des particuliers qui revendent la peluche Rakuten : Non Pixmania : Non	Auchan : Non Carrefour : Non Leclerc : Non

Nous pouvons donc remarquer que la présence de polémiques influence directement le réseau de distribution :

- **Le robot I-Que** est présent sur aucun sites spécialisés excepté « la fnac », aucun sites d'e-commerce excepté « Rakuten » et « Ebay » et aucunes GMS.
- Les **Clouds Pets**, ont complètement disparus de tous types de réseaux de distribution, tout comme **Toy-Fi Teddy**.
- Seuls les **Furby Connect** sont encore présents dans les réseaux de distribution excepté dans les magasins de jouets et les GMS.

Ces influences montrent que la pression des particuliers fait bouger les choses chez les professionnels. Le cadre juridique s'imposant moins rapidement que les nouvelles technologies, le cadre associatif et des lobbystes devient primordiales pour soulever les diverses failles de ces objets connectés. Nous pouvons dire que les particuliers essaient par différents moyens de réguler ce nouveau marché qui s'invite de plus en plus dans nos foyers.

En conclusion, nous entrons dans une ère où la sécurité et la protection des données ne sont malheureusement pas les priorités de certains acteurs sur le marché. Selon le magazine « le net expert », les cyberattaques « présentant des failles ont tendance à se multiplier ces

Document de travail. Cepe, IAE Poitiers et Ceméa. Mai 2019

derniers mois ». En effet, nous allons voir au travers de nombreux exemples, que ces nouvelles technologies nous rattrapent et que, autant les particuliers que les entreprises, nous ne sommes pas suffisamment prêts pour y faire face peu importe l'expertise que nous pouvons avoir, notamment lorsqu'il est question de jouets pour enfants ; cela rend la situation encore plus abstraite dans l'esprit de tout un chacun. Ces quatre exemples sont les plus récents mais il y en a eu d'autres comme :

- La poupée Cayla
- L'oiseau parlant Teksta Toucan
- Les lapins Karotz
- Hello Barbie
- Le dinosaure Cognitoys
- Smart Toy Bear...

Combien de jouets connectés non fiables arriveront encore sur le marché ? Pendant combien de temps les fabricants vont ignorer les normes de sécurité ?

Nous pouvons donc nous en remettre à la loi pour essayer d'encadrer les choses et déterminer des normes et des règles à respecter. Mais, quel est le rôle de la loi ? Y a-t-il vraiment un cadre sur lequel se reposer ?

III. Sur le plan national : la loi Informatique et Libertés

Les scandales relatifs à la poupée « My Friend Cayla », ou encore au robot « I-QUE » plus récemment, soulèvent de sérieuses questions quant à l'avancée du droit en matière de régulation des objets connectés destinés aux enfants âgés de moins de six ans. En 2017, la présidente de la CNIL a adressé une mise en demeure à la société GENESIS, dont la commercialisation des deux objets connectés cités précédemment provient, en raison de deux manquements à la loi Informatique et Libertés : d'une part le non-respect de la vie privée des personnes en raison d'un défaut de sécurité et d'autre part le défaut d'information des utilisateurs des jouets.

Ce cas concret révèle l'importance de la mise en place de règles juridiques notamment lorsque les objets connectés concernent directement les enfants qui sont, en ce sens, les individus les plus vulnérables.

C'est pourquoi, désormais pour des raisons de sécurité, le piratage de l'objet doit être irréalisable. Mais pour cela, les marques doivent développer des systèmes de fonctionnement adaptés à ces risques ce qui reste en soi difficilement réalisable puisqu'il s'agit d'objets dits « connectés » et que la transmission de données personnelles est automatique. Le piratage peut avoir des conséquences désastreuses dans le sens où il peut prendre plusieurs formes commençant par un simple détournement de données personnelles jusqu'à la prise de contrôle de l'objet connecté afin de s'emparer de l'ensemble de ses fonctionnalités

pour pouvoir communiquer directement avec l'enfant à des fins malveillantes.

Ces différents problèmes de piratage qui n'ont pas été anticipés par les marques qui commercialisent ce type de jouet a fait que certains pays comme l'Allemagne les ont totalement rejetés en décidant d'en interdire la vente. Une chose est sûre, pour éviter les ennuis un objet connecté destiné aux enfants doit répondre à de hautes exigences en matière de sécurité !

Il est donc désormais important d'analyser les règles juridiques qui existent à l'heure actuelle tant sur le plan national, européen ainsi qu'à l'international et d'en mesurer l'impact en termes d'usage par les tiers et également concernant la protection des données personnelles de l'enfant.

A. Le rôle de la CNIL

En France, la Commission Nationale de l'informatique et des libertés (CNIL) est une autorité administrative indépendante française en charge d'assurer la protection des données personnelles et des libertés individuelles des utilisateurs.

En ce sens, c'est elle qui doit faire respecter la loi Informatique et Libertés mise en place en France le 6 janvier 1978, soit il y a plus d'une quarantaine d'année désormais. Cette dernière est la seule règle juridique française qui encadre l'utilisation des données personnelles des utilisateurs d'internet et repose sur le principe de loyauté. Selon l'article 34 de la loi Informatique et Libertés : *« le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès »*. C'est la raison pour laquelle la CNIL imposait la déclaration de tout système de collecte de données personnelles développé par une entreprise, quel qu'il soit et dès sa création. Cette dernière pouvait également juger que cette déclaration doive se transformer en obligation d'autorisation si les données collectées étaient dites sensibles. Ces mesures préventives auprès de la CNIL ne sont pourtant plus obligatoires depuis la modification de cette loi en 2018, ce qui fait qu'elle ne détient plus un regard attentif sur tous les objets innovants qui pourraient être dotés de ce genre de système pouvant être très dangereux pour les enfants particulièrement.

B. Le principe de loyauté

La collecte des données doit être connue par l'utilisateur et nécessaire à l'usage de l'objet connecté. Une fois l'objectif atteint, ces données collectées doivent obligatoirement faire l'objet d'une suppression totale par le collecteur. Ce principe de loyauté contenu dans la loi Informatique et Libertés oblige le collecteur à la transparence et par conséquent à la sécurité des utilisateurs. Une obligation d'information davantage légitime

lorsque des enfants sont impliqués dans le processus de collecte des données personnelles afin de manière à alerter les parents.

Plus précisément, cette obligation d'information porte sur plusieurs éléments qui sont l'identité du collecteur et du destinataire, la finalité de la collecte, son caractère obligatoire ou facultatif, les conséquences d'un défaut de communication ainsi que les droits d'opposition, d'accès, de modification et de suppression des données.

C. Les sanctions relatives au non-respect de la loi

En France, le Code Pénal sanctionne le manquement à ces obligations d'une peine maximale de 5 ans d'emprisonnement et 300 000 euros d'amende pour une personne physique et ce montant peut monter jusqu'à 1 500 000 euros lorsqu'il s'agit d'une société. La CNIL peut également prononcer des sanctions administratives pouvant aller jusqu'à 300 000 euros ou bien représentant 5% du chiffre d'affaire de l'entreprise en cas de réitération du non-respect de la loi dans les 5 ans qui suivent la sanction.

D. Au niveau européen : Le RGPD

D.1. Les principes de « Privacy by design and default »

Sur le plan européen, aucune législation n'était en vigueur avant 2018 avec la signature du règlement général de la protection des données pour tous les États membres. Tandis qu'en France, la loi Informatique et libertés s'appuie sur le principe de loyauté, le RGPD lui consacre deux autres principes dénommés « Privacy by design » ainsi que « Privacy by default ». Le premier implique que l'objet connecté doit assurer la confidentialité des données transmises par l'utilisateur dès sa création et ce, pour pallier les risques de sécurité qui ont déjà été encourus après la commercialisation de certains produits connectés par certains enfants. Le second principe repose sur le fait que les données personnelles nécessaires à l'utilisation de l'objet connecté doivent être moindres de façon à assurer un très haut niveau de sécurité aux consommateurs. Ces deux principes contenus dans le RGPD affirment la volonté des États d'autoriser la commercialisation de produits connectés plus sécurisés à l'avenir pour éviter les mauvaises surprises de la part de certaines entreprises qui n'y prêtent pas assez d'attention.

D.2. Le droit à l'oubli numérique et la majorité numérique

D'autre part, le RGPD renforce le droit à l'oubli numérique c'est-à-dire qu'il donne la possibilité à l'utilisateur de demander l'effacement de ses données personnelles préalablement transmises à l'objet. Mais pour cela, sa requête doit répondre à plusieurs critères qui sont le fait que les données ne sont plus nécessaires à l'utilisation de l'objet, que le délai de conservation autorisé est arrivé à expiration ou bien que le consommateur ait décidé de retirer son consentement quant à la préservation de ses données personnelles. Il est tout de même important de souligner que ce droit à l'oubli numérique connaît des exceptions dans le cadre d'une

recherche scientifique ou la révélation de crimes et délits si l'utilisateur se trouve impliqué dans les faits.

Avant l'élaboration de ce règlement, il existait un grand vide juridique concernant la protection des données personnelles en général sur le plan européen et notamment sur la condition des mineurs. Le manque de législation de ce côté-là faisait que le principe de la majorité numérique s'appliquait dans tous les cas de figure. Or depuis 2018, une collecte de données personnelles concernant un enfant de moins de 16 ans nécessite l'autorisation préalable de ses parents ou de ses responsables légaux. Il existe toutefois une nuance à cette règle juridique qui autorise les États membres de l'Union européenne à abaisser cet âge tant qu'il reste inférieur à 13 ans. La majorité numérique n'est donc pas homogène selon les pays. En ce qui concerne le cas de la France, cette dernière a fixé cette majorité numérique à 15 ans selon la loi du 20 juin 2018 relative à la protection des données personnelles qui est venue modifier la loi Informatique et Libertés de 1978.

D.3. Les sanctions relatives au non-respect du règlement

En France, le RGPD a permis de renforcer les contrôles dans les entreprises notamment sur son degré de sécurité et va même jusqu'à imposer la désignation d'un délégué à la protection des données personnelles directement dans certaines entreprises afin de faire respecter la législation européenne et française en vigueur et ainsi d'éviter les sanctions de la CNIL. En termes de chiffres, le règlement prévoit une amende qui peut s'élever à 20 millions d'euros ou à 4% du chiffre d'affaire mondial de l'entreprise en cas de non-respect de la législation en matière de protection des données personnelles des consommateurs engageant la responsabilité du concepteur et de ses sous-traitants également.

Il est important de souligner sur le RGPD n'est pas assez développé pour assurer la sécurité des objets connectés, cette législation au niveau européen est encore insuffisante. Le Bureau européen des unions de consommateurs allant jusqu'à qualifier ce manque de contrôle législatif tel un « trou béant dans la législation européenne ».

E. L'exemple de la Californie à l'international

Du côté de la Californie, une loi spécialement dédiée à réguler les objets connectés entrera en vigueur d'ici 2020. Cette dernière impose que les fabricants de tels objets répondent à des critères de sécurité renforcés. En effet, les données collectées dans le cadre de l'utilisation de ces objets devront être totalement inaccessibles à des personnes tierces pour éviter les risques de piratage à distance et ne pourront pas faire l'objet d'une quelconque divulgation. Ce contrôle renforcé en matière de collecte de données personnelles via des objets connectés se fera à l'aide de la création d'un mot de passe personnalisé choisi par l'utilisateur. Cette loi met en avant l'avancée du droit californien sur ce sujet précis et il est également prévu qu'à l'horizon 2020, un équivalent du RGPD européen

viendra s'ajouter à la législation actuelle pour renforcer la sécurité des consommateurs friands de ces objets toujours plus innovants. Cette loi californienne a pour objectif d'avoir un impact à l'échelle mondiale afin que l'ensemble des États prennent des mesures similaires en matière de régulation des objets connectés. Une avancée juridique bénéfique qui pourrait inspirer l'Europe dans les années à venir...

En conclusion, nous pouvons remarquer que le cadre législatif est encore moindre par rapport aux polémiques que soulèvent les objets connectés. D'ailleurs, il y a une inexistence de textes, de lois, d'encadrement par rapport aux problèmes que ces objets ont sur la santé et le développement de l'enfant.

IV. Les Normes : un cadre qui évolue

A. Normes liées à l'aspect physique

L'Europe et la France en particulier ont renforcé les normes les normes de fabrication et de sécurité des jouets. La directive européenne 2009/48/CE impose aux fabricants de procéder à une analyse des risques de leurs produits avant leur commercialisation.

Selon le site de la direction générale des Entreprises³⁵ qui appartient au ministère de l'économie et de Finance ; les jouets sont réglementés en France par le décret n° 2010-166 du 22 février 2010 et son arrêté d'application du 24 février 2010. Ces textes transposent la nouvelle directive européenne 2009/48/CE relative à la sécurité des jouets qui est entrée en vigueur sur tout le territoire de l'Union européenne le 20 juillet 2011 et le 20 juillet 2013 pour les exigences spécifiques à la chimie.

Pour faciliter l'application des textes réglementaires, des normes dites harmonisées avec les textes réglementaires ont été développées.

Elles donnent présomption de conformité, c'est-à-dire que tout produit conforme aux normes respecte nécessairement la réglementation. Toutes les informations sur ces normes peuvent être obtenues sur le site d'AFNOR.

Parmi ces normes on trouve notamment la **Norme NF EN71. 1** lié aux propriétés physiques et mécaniques, **la norme NF EN71.2** concernant l'Inflammabilité, et **la norme NF EN71.3** liée aux propriétés chimiques.

B. Normes liées à la sécurité des jouets électriques

³⁵ Entreprises. Gouv : <https://www.entreprises.gouv.fr/politique-et-enjeux/qualite/securite/la-reglementation-applicable-aux-jouets>

Norme NF EN 62115/A12 Février 2018 pour la sécurité des jouets électriques :

“Les jouets devant être alimentés en très basse tension de sécurité (TBTS), n’entrent pas dans le champ d’application de la DBT. Si le jouet comporte un chargeur externe alimenté sur le secteur, le chargeur seul relève de la DBT.

Si ce jouet intègre des éléments électroniques actifs, il relève également de la réglementation concernant la compatibilité électromagnétique.”³⁶

Une autre obligation pour les entreprises, il s’agit d’avertissement de sécurité. Selon le site de la Direction Générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF) : *“les jouets destinés aux enfants de moins de 3 ans munis de câbles électriques de plus de 300 mm de long et les jouets destinés aux enfants entre 18 mois et 3 ans munis de câbles électriques de plus de 200 mm de long, ainsi que leur emballage, doivent porter l’avertissement : Attention ! Ne convient pas aux enfants de moins de 18 mois (exemple : corde et chaîne longue, câble long = danger de strangulation).”³⁷*

D’autre part, en analysant le packaging des jeux et jouets des enfants, il existe des labels ou marques qui renvoient aux respects des normes de fabrication par le producteur de ce jeu ou jouet.

Parmi ces labels, nous relevons le fameux marquage “CE” :³⁸

Le logo "CE" indique que le fabricant déclare que le produit est conforme aux exigences de la réglementation européenne. Ces exigences tournent autour de trois aspects : propriétés mécaniques et physiques, inflammabilité et migration de substances chimiques. Cependant, ce marquage est apposé sous la propre responsabilité du fabricant et n'est donc fiable que si ce dernier est de bonne foi.



Des labels spécifiques pour prouver l’innocuité chimique :

³⁶ Entreprises. Gouv : <https://www.entreprises.gouv.fr/politique-et-enjeux/materiels-electriques-et-electroniques>

³⁷ Entreprises. Gouv : <https://www.economie.gouv.fr/dgccrf/Publication/Vie-pratique/Fiches-pratiques/jouets-electriques>

³⁸ Les pros de la petite enfance : <https://lesprosdela petiteenfance.fr/equipements-produits/jeux-et-jouets/securite-des-jouets-tout-ce-que-vous-devez-savoir/jouets-les-normes-et-labels-connaître>

Les plastiques, mousses, textiles peints, peinture ou encore vernis qui composent certains jouets peuvent s'avérer dangereux pour la santé des enfants.

Cependant, la réglementation interdit dans les jouets susceptibles d'entrer en contact avec la bouche, les produits de maquillage pour enfants, les feutres, la peinture... une vingtaine de composants (plomb, aluminium, chrome, cadmium...) au-delà de certaines teneurs.

Pour plus de sécurité, le fabricant peut opter pour le label "Oeko-Tex" qui garantit que le jouet, essentiellement les peluches et les doudous, ne contient aucun produit chimique nocif pour la peau (métaux lourds, formaldéhyde, phtalates). Par ailleurs, les labels FSC et PEFC attribués aux jouets et jeux en bois soulignent que l'approvisionnement en bois tient compte de la gestion durable des ressources forestières.



Dans notre analyse, nous avons trouvé que les jouets connectés destinés aux enfants sont tous conformes aux normes de fabrication liés aux propriétés physiques, mécaniques ainsi que les normes de sécurité électroniques et les avertissements de sécurité liés à l'âge convenable des enfants.

Toutefois, ceci ne s'applique pas aux enjeux liés à la sécurité électronique, à la cybersécurité ou à la protection de la vie privée des enfants car il s'agit de collecte de données personnelles comme des dossiers sons, des images et des noms via des objets ou Jouets connectés ; Nous n'avons pu trouver de vrais règles ou normes en vigueur qui puissent les protéger.

L'Union européenne a fait un pas de plus vers l'adoption de nouvelles règles sur la certification et la coopération entre les pays en matière de cybersécurité. Le comité de l'industrie du Parlement européen a ratifié le Cybersecurity Act.³⁹ Pourtant, le Parlement ne souhaite rendre les certifications obligatoires que pour les produits et services technologiques présentant les risques de sécurité les plus élevés.

39 Zdnet : <https://www.zdnet.fr/actualites/securite-des-objets-connectes-un-trou-beant-dans-la-loi-39871033.htm>

Ces certifications sont susceptibles de concerner des domaines comme l'infrastructure énergétique. Les détails doivent encore être débattus lors des négociations.

Nous arrivons donc à une situation où la “sécurité est non impérative = négligée”. Des cas de faille documentées sont mises en valeurs mais les autorités sont toujours en retard par rapport aux faits réels. Des problèmes liés aux botnets⁴⁰ d'objets connectés inquiète beaucoup les associations concernées par la protection du consommateur. L'émergence de botnets comme Mirai a également démontré le danger présenté par la multitude de ces terminaux non sécurisés. Selon les experts les risques sont multiples, allant du vol à la manipulation des données.

C'est pourquoi les associations de protection demandent - depuis longtemps - aux institutions européennes d'imposer des exigences en matière de cybersécurité, comme des mises à jour de sécurité, des mots de passe forts ou du chiffrement pour les montres, les voitures connectées et autres réfrigérateurs intelligents.

Quelles solutions ?

Il est primordial que les constructeurs d'appareils et les entreprises qui les exploitent prennent en compte la sécurité dès le début de la fabrication d'un produit. Il est essentiel de pouvoir établir un dialogue entre experts en sécurité et développeurs d'appareils informatiques pour maisons connectées. Il est également important que la législation avance par rapport à ce sujet vu la vulnérabilité des parties concernées notamment les enfants.

Ici encore, aucunes normes sur la santé ne sont évoquées.

V. Des petits conseils pour parents

En attendant que la loi contribue à une véritable protection de la vie privée des consommateurs et que nous puissions avoir un vrai changement vis-à-vis la situation actuelle.

Voici quelques conseils pour se prémunir face à ces potentielles attaques. Dans le meilleur des cas, les microphones, les appareils photo et les dispositifs de localisation peuvent être désactivés afin de freiner les pirates, mais il existe quelques vulnérabilités logicielles contre lesquelles l'utilisateur ne peut pas faire grand-chose. Quelques actions indispensables sont tout de même possibles comme de vérifier que le jouet a été acheté auprès d'une source de confiance, d'étudier la politique de sécurité du fabricant, de modifier les identifiants

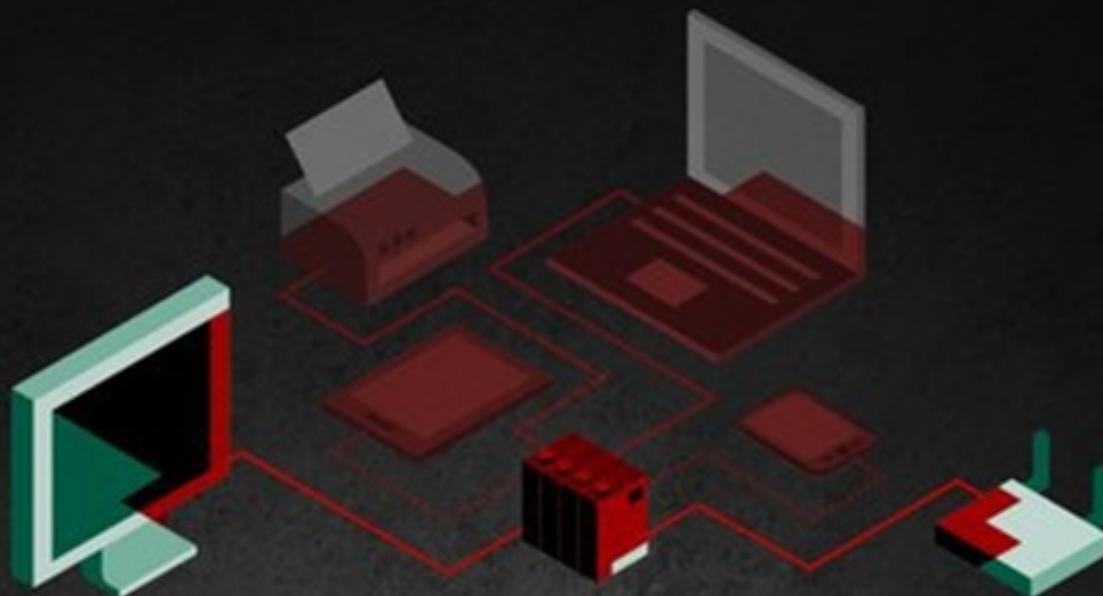
40 Termes américains qui est une contraction de « robot » et « réseau ». C'est un réseau de bots informatiques, des programmes connectés à Internet qui communiquent avec d'autres programmes similaires pour l'exécution de certaines tâches.

par défaut par un nouveau nom d'utilisateur et un mot de passe fort, et d'activer l'authentification à deux facteurs. Et devant la prolifération des objets connectés au sein du foyer, l'idéal est de mettre en place une solution de sécurité globale tels qu'un box de sécurité pour toute la maison permettant de protéger de la même manière l'ensemble des objets connectés à Internet contre les malwares, les usurpations d'identité et les failles de sécurité.

Un expert interrogé sur le sujet, répond : "La première chose est de lister tous les objets connectés de la maison et de savoir comment et à quoi ils sont connectés (à Internet, ou à d'autres objets de la maison). Ensuite, il est impératif de mettre des obstacles sur la route du hacker. Pour ce faire, il faut tout d'abord installer régulièrement les mises à jour de sécurité et les mises à jour logicielles, pour limiter le nombre de vulnérabilités connues qui pourraient être exploitées. Après, il faut changer le nom et le mot de passe par défaut de chaque objet connecté, car c'est la première chose qu'un hacker tentera d'attaquer pour en prendre le contrôle. Pour finir, il faut limiter l'accès d'un objet connecté aux autres objets connectés dans la maison.

Enfin, en poursuivant la sensibilisation autour de la sécurité en général, et notamment des jouets et objets connectés, nous en tant qu'utilisateurs allons également gagner en vigilance et en compétences, pour être progressivement capables de s'éloigner des produits n'inspirant pas confiance au profit de produits plus respectueux..."

The dark side of your living room



Smart TV

- No encryption: scammers could steal your money while you try to buy content via the TV
- Smart TVs execute Java code, making it possible to launch exploit-driven attacks

Network attached storages

- Devices have weak default passwords
- Malicious files can be uploaded into NAS
- NAS can infect other connected devices
- It can be shackled to a botnet

DSL router

- An Internet Service Provider can get remote access to any device in your network

How to stay safe in the world of connected devices

1 Utilize the latest security and firmware updates

2 Change all default usernames and passwords

3 Restrict access to devices: there's no real reason to connect a printer to your TV

Conclusion

D'un point de vue juridique, même si l'apparition des objets connectés est relativement récente, les textes de loi ont mis du temps à réellement encadrer leur utilisation et régler les problèmes liés à la protection des données personnelles des consommateurs. Il a fallu attendre la survenue de quelques scandales pour que les autorités législatives s'emparent de la question et donnent un cadre à l'activité technologique. Cependant, aucune loi ne régit encore spécialement tous les aspects des objets connectés comme le droit californien par exemple. C'est pourquoi, les États européens ont encore des progrès à faire en matière juridique pour assurer une réelle sécurité aux utilisateurs et protéger les enfants lorsqu'il s'agit de technologie infantile.

En matière d'éthique, les objets connectés posent de sérieux problèmes en ce qui concerne l'atteinte à la vie privée de l'utilisateur. Et cette immersion dans la vie privée des individus grâce à la collecte des données personnelles est d'autant plus dangereuse lorsque l'objet connecté cible un enfant de moins de 6 ans comme c'est le cas pour beaucoup de jouets robotiques. Nous entrons dans une ère où la sécurité et la protection des données ne sont malheureusement pas les priorités de certains acteurs sur le marché des objets connectés. Selon le magazine Le Net Expert, les cyberattaques « présentent des failles et ont tendance à se multiplier ces derniers mois ». Nous avons vu à travers de nombreux exemples d'actualité que ces nouvelles technologies infantiles vont plus vite que le droit qui est censé les réguler. Que ce soit en tant que particuliers ou professionnels, nous ne sommes pas suffisamment prêts pour faire face à l'évolution de l'innovation si rapide en matière d'objets connectés malgré l'expertise que nous pouvons avoir dans ce domaine. Pour ce qui est de ceux qui sont destinés aux enfants, cela reste encore abstrait dans l'esprit des consommateurs dans le sens où ils ne se rendent pas vraiment compte des risques concernant la collecte d'information personnelles mais aussi envers leur santé dû aux ondes générées par la connexion que ces objets requièrent. En prenant l'exemple de la poupée Cayla, l'oiseau parlant Teksta Toucan, les lapins Karotz, Hello Barbie, Le dinosaure Cognitoys ou encore Smart Toy Bear... Nous pouvons nous demander combien de jouets connectés non fiables comme ceux-là parviendront-ils à se faire une place sur le marché ? Pendant combien de temps les fabricants vont-ils encore ignorer l'ensemble des normes de sécurité pourtant obligatoires à la fois dans la loi française et également au niveau européen ? Il est donc impératif de renforcer le cadre légal dans cette matière-là pour donner plus de visibilité aux risques engendrés par ces

objets connectés à la fois aux consommateurs qu'aux professionnels. Les produits de l'enfant connectés sont souvent développés pour répondre aux anxiétés parentales de plus en plus présentes chez les parents d'aujourd'hui, complètement désorientés face aux technologies infantiles. Pour vendre ce type de produit, les fabricants d'objets connectés destinés aux enfants développent un discours marketing particulier qui insiste sur le fait de palier à coup sûr les inquiétudes des parents en dotant l'objet d'un caractère indispensable pour être de « bon parents » à cette époque, alors que la plupart d'entre eux sont nocifs pour leur famille...

Webographie

- **Les objets connectés entre solutions et enjeux**

iBaby - See Your Baby With The Best Wi-Fi Video Baby Monitors. (s.d.). *iBaby*. Repéré 24 janvier 2019, à <https://ibabylabs.com/>

Michel, A. (s.d.). *Copain ? - Charlotte Gastaut*. Repéré à <https://www.albin-michel.fr/ouvrages/copain-9782226325150>

Objets connectés et vie quotidienne : où en sommes nous ? (2018, 25 octobre). *Laboratoire d'Analyse et de Décryptage du Numérique*. Repéré à <https://labo.societenumerique.gouv.fr/2018/10/25/objets-connectes-vie-quotidienne-sommes/>

Playful and Smart Toothbrushes For Families. (s.d.). Repéré 24 janvier 2019, à <https://www.kolibree.com/fr/families/>

Privacy Policy. (s.d.). Repéré 24 janvier 2019, à https://www.kolibree.com/fr/privacy_policy/

What are the Best IoT-Based Children Safety Devices? - Meee Services. (2018, 4 septembre). *MEEE*. Repéré à <https://meee-services.com/what-are-the-best-iot-based-children-safety-devices/>

- **Les objets connectés et leurs multiples polémiques**

Attention, votre jouet connecté pourrait être piraté. (s.d.). *LCI*. Repéré 24 janvier 2019, à <https://www.lci.fr/societe/jt-20h-les-jouets-connectes-peuvent-ils-etre-hackes-2019261.html>

cloudpetssignonletter.pdf. (s.d.). Repéré à <https://www.eff.org/files/2018/05/28/cloudpetssignonletter.pdf>

Correspondent, R. S. C. affairs. (2017, 14 novembre). Strangers can talk to your child through « connected » toys, investigation finds. *The Guardian*. Repéré à <https://www.theguardian.com/technology/2017/nov/14/retailers-urged-to-withdraw-toys-that-allow-hackers-to-talk-to-children>

[Infographie] Il était une fois l'ours connecté mal sécurisé | CNIL. (s.d.). Repéré 24 janvier 2019, à <https://www.cnil.fr/fr/infographie-il-etait-une-fois-lours-connecte-mal-securise>

Jouets connectés – Trop faciles à détourner. (s.d.). Repéré 24 janvier 2019, à <https://www.quechoisir.org/actualite-jouets-connectes-trop-faciles-a-detourner-n46276/>

Jouets connectés : des peluches piratées pour récupérer des données personnelles. (s.d.). *Génération-NT*. Repéré 24 janvier 2019, à <https://www.generation-nt.com/jouets-connectes-peluches-pirates-recuperation-800-000-comptes-donnees-personnelles-actualite-1940050.html>

Jouets connectés : la CNIL met en demeure le fabricant de la poupée Cayla et du robot I-Que. (2017, 4 décembre). Repéré à https://www.lemonde.fr/pixels/article/2017/12/04/jouets-connectes-la-cnil-met-en-demeure-le-fabricant-de-la-poupee-cayla-et-du-robot-i-que_5224291_4408996.html

Le jouet intelligent, le cadeau de Noël idéal... pour les pirates ! (2018, 17 décembre). *Programmez!* Repéré 24 janvier 2019, à <https://www.programmez.com/avis-experts/le-jouet-intelligent-le-cadeau-de-noel-ideal-pour-les-pirates-28363>

Les données personnelles de 800 000 propriétaires d'ours en peluche connectés accessibles sur Internet. (2017, 28 février). Repéré à https://www.lemonde.fr/pixels/article/2017/02/28/les-donnees-personnelles-de-800-000-proprietaires-d-ours-en-peluche-connectes-accessibles-sur-internet_5087012_4408996.html

Ng, A. (s.d.). Amazon will stop selling connected toy filled with security issues. *CNET*. Repéré 24 janvier 2019, à <https://www.cnet.com/news/amazon-will-stop-selling-connected-toy-cloud-pets-filled-with-security-issues/>

Objets connectés : Bienvenue dans le royaume de l'inutile et de la poudre aux yeux. (2018, 17 août). *Maddyness - Le Magazine sur l'actualité des Startups Françaises*. Repéré 24 janvier 2019, à <https://www.maddyness.com/2018/08/17/iot-objets-connectes-inutile/>

Orsini, A. (2017, 14 novembre). Furby, robots i-Que : la sécurité de certains jouets connectés pose toujours problème - Tech. *Numerama*. Repéré 24 janvier 2019, à <https://www.numerama.com/tech/305902-furby-robots-i-que-la-securite-de-certains-jouets-connectes-pose-toujours-probleme.html>

Prévost, T. et Simon, M. (2017, 16 novembre). Pour Noël, offrez des jouets connectés vulnérables à vos gamins. *Motherboard*. Repéré à <https://motherboard.vice.com/fr/article/evb77j/pour-noel-offrez-des-jouets-connectes-vulnerables-a-vos-gamins>

Safety alert: see how easy it is for almost anyone to hack your child's connected toys. (2017, 14 novembre). *Which? News*. Repéré 24 janvier 2019, à <https://www.which.co.uk/news/2017/11/safety-alert-see-how-easy-it-is-for-almost-anyone-to-hack-your-childs-connected-toys/>

Alerte sur le danger des jouets espions avant les fêtes de Noël - 05/12/2017 - midilibre.fr. (s.d.). Repéré 24 janvier 2019, à <https://www.midilibre.fr/2017/12/05/vie-privee-alerte-sur-le-danger-des-jouets-connectes-avant-noel,1598354.php>

- **Sur le plan national : la loi Informatique et Libertés**

Avocats, M. (2018, 30 octobre). Objets connectés: nouvelle loi californienne. *Mathias Avocats*. Repéré à <https://www.avocats-mathias.com/actualites/californie-loi-objets-connectes>

Décision MED-2017-073 du 20 novembre 2017.

Délibération de la Commission Nationale de l'Informatique et des Libertés. , 2017-295 (2017).

Jouets connectés : mise en demeure publique pour atteinte grave à la vie privée en raison d'un défaut de sécurité | CNIL. (s.d.). Repéré 24 janvier 2019, à <https://www.cnil.fr/fr/jouets-connectes-mise-en-demeure-publique-pour-atteinte-grave-la-vie-privee-en-raison-dun-defaut-de>

Juillet 2018, P. D. M. | M. 11. (s.d.). Sécurité des objets connectés : un « trou béant » dans la loi. *ZDNet France*. Repéré 24 janvier 2019, à <https://www.zdnet.fr/actualites/securite-des-objets-connectes-un-trou-beant-dans-la-loi-39871033.htm>

LABBE, +Pierrick. (2018, 1 octobre). La Californie passe une loi pour la sécurité des objets connectés. *OBJETCONNECTE.NET*. Repéré à <https://www.objetconnecte.net/californie-loi-securite-objets-connectes/>

Lausson, J. (2017, 4 décembre). Jouets connectés : la Cnil épingle les failles de sécurité du robot i-Que et de la poupée Cayla - Politique. *Numerama*. Repéré 24 janvier 2019, à <https://www.numerama.com/politique/311501-jouets-connectes-la-cnil-epingle-les-failles-de-securite-du-robot-i-que-et-de-la-poupee-cayla.html>

Objets connectés : législation et précautions - Ooreka. (s.d.). *Ooreka.fr*. Repéré 24 janvier 2019, à [//domotique.ooreka.fr/astuce/voir/297537/legislation-autour-des-objets-connectes](http://domotique.ooreka.fr/astuce/voir/297537/legislation-autour-des-objets-connectes)

- **Les normes : un cadre qui évolue & Des petits conseils pour parents**

[Infographie] Il était une fois l'ours connecté mal sécurisé | CNIL. (s.d.). Repéré 24 janvier 2019, à <https://www.cnil.fr/fr/infographie-il-etait-une-fois-lours-connecte-mal-securise>

Jouets connectés : quels conseils pour les sécuriser ? | CNIL. (s.d.). Repéré 24 janvier 2019, à <https://www.cnil.fr/fr/jouets-connectes-quels-conseils-pour-les-securiser>

Jouets : les normes et labels à connaître. (2016, 22 février). *lesprodelapetiteenfance*. Repéré 24 janvier 2019, à <https://lesprodelapetiteenfance.fr/equipements-produits/jeux-et-jouets/securite-des-jouets-tout-ce-que-vous-devez-savoir/jouets-les-normes-et-labels-connaître>

Juillet 2018, P. D. M. | M. 11. (s.d.). Sécurité des objets connectés : un « trou béant » dans la loi. *ZDNet France*. Repéré 24 janvier 2019, à <https://www.zdnet.fr/actualites/securite-des-objets-connectes-un-trou-beant-dans-la-loi-39871033.htm>

La réglementation applicable aux jouets. (s.d.). *Direction Générale des Entreprises (DGE)*. Repéré 24 janvier 2019, à <https://www.entreprises.gouv.fr/politique-et-enjeux/qualite/securite/la-reglementation-applicable-aux-jouets>

Les PKI, la solution de sécurité pour les objets connectés. (s.d.). *Global Security Mag Online*. Repéré 24 janvier 2019, à <http://www.globalsecuritymag.fr/Les-PKI-la-solution-de-securite,20180619,79317.html>

Objets connectés : législation et précautions - Ooreka. (s.d.). *Ooreka.fr*. Repéré 24 janvier 2019, à [//domotique.ooreka.fr/astuce/voir/297537/legislation-autour-des-objets-connectes](http://domotique.ooreka.fr/astuce/voir/297537/legislation-autour-des-objets-connectes)
(S.d.). Repéré à <https://m.boutique.afnor.org/recherche/resultats/mot/Jouet/categorie/normes>