Contrôle des objets connectés

Après avoir brièvement résumé les documents ci-dessous, vous expliquerez les risques encourus par l'utilisateur·ice d'un objet connecté si cet objet est contrôlé par le fabriquant plutôt que par l'utilisateur·ice.

Document 1 : *Lorsque Google arrête Revolv, sa box domotique, le monde de l'IoT en pâtit, Hervé, http://www.abavala.com, 8/04/2016*[1].

> L'histoire de Revolv avait pourtant bien commencé. Très bien même. Cette solution pour la Smart Home avait tout pour plaire : ergonomique, multiprotocole, intégrant bon nombre de produits connectés, … […] Pendant ce temps là, Google a racheté Nest pour en faire son fer de lance pour la Smart Home. Puis Nest à racheté Revolv. Et Nest décide d'arrêter l'aventure Revolv. La fin est annoncée pour mai 2016.
> […]
> Les clients de la solution ont reçu une information leur indiquant que le service Revolv cessera dès le 15 mai 2016. […] Dans le cas de Revolv, la pilule passe mal. Ils ne faut pas oublier que les clients de la solution ne bénéficient pas gratuitement du service : ils ont déboursé 300$ pour acheter cette box domotique qui dans un mois ne servira plus à rien car Nest a décidé d'arrêter les serveurs qui sont un élément vital de la solution en même temps que la solution elle même.
> […]
> Ce qui est reproché outre atlantique n'est au final que l'application des "Terms of services", ces fameuses petites lignes que l'on ne lit jamais avant d'acheter ou d'activer un service ou un produit. Ils stipulaient que Revolv se réservait le droit d'interrompre le service après en avoir informé les clients. C'est ce qu'ils font aujourd'hui.

Document 2 : *The maker of an internet-connected garage door disabled a customer's device over a bad review, Rob Price, Business Insider, 5 avril 2017*[2] *(traduction de Louis Paternault).*

> Utiliser des gadgets connectés présente un nouveau risque dystopique : si vous vous plaignez, le fabriquant peut bloquer votre produit.
>
> C'est ce qui est arrivé à un client de Garadget — une porte de garage connectée. Elle permet de verrouiller ou déverrouiller la porte à distance avec une application, ou voir si elle est ouverte.

1 https://www.abavala.com/lorsque-google-arrete-revolv-box-domotique-monde-de-l-iot-patit/
2 https://www.businessinsider.fr/us/iot-garage-door-opener-garadget-kills-customers-device-bad-amazon-review-2017-4

Mais après s'être plaint en ligne, et avoir laissé un avis négatif, il a eu une mauvaise surprise — Garagdet a bloqué son appareil. […]

Le client avait laissé un commentaire sur le forum d'assistance pour se plaindre de problèmes techniques, demandant « quelle merde je viens d'acheter. » Il avait ensuite laissé un avis négatif sur Amazon […].

Garadget n'a pas apprécié cette partie là.

L'entreprise a désactivé l'appareil du client mécontent, en lui interdisant l'accès à ses serveurs […].

Objets connectés et Vie privée

Après avoir brièvement résumé le document ci-dessous, vous expliquerez comment les objets connectés peuvent aider des entreprises ou des personnes mal intentionnées à violer la vie privée des utilisateur·ice·s.

Document 1 : *Sécurité : la Cnil accuse deux jouets connectés d'atteinte grave à la vie privée des enfants, Lucie Ronfaut, lefigaro.fr, 04/12/2017*[1].

Lundi, la Cnil a mis en demeure la société Genesis Industries, fabricant hongkongais de deux jouets connectés, pour « atteinte grave à la vie privée en raison d'un défaut de sécurité ». Il s'agit du robot i-Que et de la poupée Cayla, qui sont tous les deux commercialisés en France. « Ces vérifications ont permis de relever que la société collecte une multitude d'informations personnelles sur les enfants et leur entourage : les voix, le contenu des conversations échangées avec les jouets (qui peut révéler des données identifiantes comme une adresse, un nom…) mais également des informations renseignées dans un formulaire [d'une application] », précise l'autorité.

[…]

Les jouets intelligents peuvent poser plusieurs problèmes de sécurité. […] Par exemple, il est reproché au robot i-Que et à la poupée Cayla de ne pas sécuriser la connexion Bluetooth nécessaires pour les faire fonctionner. N'importe qui pouvait utiliser son smartphone pour se connecter au jouet, et donc le contrôler, sans remplir un code d'accès ou un mot de passe. On peut aussi les utiliser pour communiquer avec les enfants, en appelant le téléphone connecté ou en diffusant des sons pré-enregistrés. « Les contrôleurs de la CNIL ont constaté qu'une personne située à 9 mètres des jouets à l'extérieur d'un bâtiment, peut connecter (ou « appairer ») un téléphone mobile aux jouets grâce au standard de communication Bluetooth sans avoir à s'authentifier », note la Cnil.

[…]

« Ce ne sont pas des problèmes simples à détecter, c'est difficile de s'en rendre compte soi-même », juge Justine Massera, juriste chez UFC Que-Choisir. Leurs conséquences peuvent pourtant être graves. En 2015, un internaute est parvenu à récupérer les données personnelles de cinq millions de parents et de 6 millions de jeunes propriétaires de jouets fabriqués par VTech. Parmi ces informations personnelles, des photos d'enfants. Plus récemment, en 2017, les peluches de Spiral Toys ont également été victimes d'une grave faille de sécurité, rendant accessibles plus de 200.000 enregistrements vocaux d'enfants.

1 http://www.lefigaro.fr/secteur/high-tech/2017/12/04/32001-20171204ARTFIG00098-securite-la-cnil-accuse-deux-jouets-connectes-d-atteinte-grave-a-la-vie-privee-des-enfants.php

Document 2 : *Elle a installé une caméra Ring dans la chambre de ses enfants pour sa « tranquillité d'esprit ». Un hacker y a accédé et a harcelé sa fille de huit ans, Allyson Chiu, The Washington Post, 12/12/2019*[2]*.*

Dans un échange glaçant capturé en vidéo la semaine dernière, les LeMay racontent [qu'un étranger] a pu interagir avec leur fille après avoir piraté une caméra de vidéosurveillance Ring qui avait été installée récemment dans la chambre partagée par Alyssa et ses deux petites sœurs. Durant plusieurs minutes, l'homme a proféré des insultes racistes à son encontre, et a essayé de la persuader de faire des bêtises [...].

Les LeMay, pourtant, ne sont pas les seules personnes à avoir vécu ce cauchemar ces dernières semaines. Plusieurs utilisateurs dans tous le pays on raconté que leur système de sécurité a aussi été infiltré par des pirates qui les ont harcelés grâce à la fonction de discussion de la caméra.

2 https://www.washingtonpost.com/nation/2019/12/12/she-installed-ring-camera-her-childrens-room-peace-mind-hacker-accessed-it-harassed-her-year-old-daughter/

Informatique biaisée

Après avoir brièvement résumé les documents ci-dessous, vous expliquerez pourquoi des personnes qui ne sont pas discriminantes (ni racistes, ni sexistes, etc.) peuvent créer des systèmes discriminants, et quelles solutions permettraient d'éviter ce genre de problèmes.

Document 1 : *This Viral Video Of A Racist Soap Dispenser Reveals A Much, Much Bigger Problem, Tom Hale, IFLScience!, 18/08/2017*[1] *(traduction de Louis Paternault).*

Chukwuemeka Afigbo, un nigérien travaillant dans la technologie, a twitté une courte vidéo d'un distributeur de savon « raciste », qui donne du savon dans la main d'une personne blanche, mais pas dans celle d'une personne noire. […]

Ce problème simple aurait été évité si le distributeur avait été testé sur différents teints de peaux. […]

Il existe beaucoup d'exemples similaires. […] Par le passé, Flickr et Google avaient tous les deux été obligé de présenter leur excuses lorsque leurs systèmes automatiques de reconnaissance d'images classaient des photos de personnes noires comme « singe » ou « gorille ». […]

Une étude scientifique a aussi mis en lumière le problème des applications de reconnaissance vocale beaucoup plus efficaces pour comprendre les voix masculines plutôt que les féminines. La raison étant que le logiciel avait été entraîné principalement avec les voix d'hommes. […]

De prime abord, ces petites bourdes comme le distributeur de savon peuvent paraître drôles : comment une machine sans conscience pourrait-elle être raciste ? Mais en réalité, elles montrent simplement pourquoi la diversité est si importante. Après tout, l'entreprise derrière le distributeur n'était probablement pas volontairement raciste. Néanmoins, elle a été indélicate.

Document 2 : *Les personnes noires auraient plus de risques de se faire renverser par une voiture autonome, Sophie Kloetzli, Usbek & Rica, 04/03/2019*[2]*.*

Des chercheurs du Georgia Institute of Technology à Atlanta aux États-Unis ont mis en évidence les biais racistes des systèmes de reconnaissance. La détection de piétons à la couleur de peau foncée serait moins précise que pour les personnes blanches.

[…]

C'est du moins la conclusion d'un nouveau rapport publié le 21 février par une équipe de chercheurs américains. Ceux-ci ont confronté huit systèmes de

1 https://www.iflscience.com/technology/this-racist-soap-dispenser-reveals-why-diversity-in-tech-is-muchneeded/

2 https://usbeketrica.com/article/personnes-noires-chances-renverser-voitures-autonomes

reconnaissance (sans préciser lesquels) à plusieurs dizaines de milliers d'images de piétons prises à New York, Berkeley, San Francisco et San Jose, et dans diverses conditions météorologiques. Les résultats indiquent que les algorithmes de détection existants sont généralement moins performants lorsqu'il s'agit d'identifier des personnes noires.

« Les erreurs faites par les voitures autonomes pourraient être inégalement réparties dans les différents groupes démographiques », alertent-ils. Autrement dit, ces véhicules pourraient avoir plus de faciliter à détecter, et donc à esquiver, les piétons blancs que les piétons noirs.

[…]

« La base de données d'apprentissage contient environ 3,5 fois plus d'exemples de piétons des catégories 1 à 3 [à la peau claire, NDLR] », détaillent les chercheurs. Cette disparité serait ainsi à leurs yeux la raison principale des biais racistes des systèmes de détection. Une base de données plus fournie et plus inclusive conduisent logiquement à une reconnaissance plus fine des individus.

Informatique embarquée et Sécurité

Après avoir brièvement résumé les documents ci-dessous, vous expliquerez s'il est possible de créer des systèmes embarqués sans aucune faille, et ce qu'il faudrait alors faire pour prévenir les conséquences de telles failles.

Document 1 : *Le protocole Z-Wave met votre maison connectée à la portée des pirates, Gilbert Kallenborn, 01net.com, 28/05/2018*[1]*.*

> Si vous utilisez des serrures interconnectées au travers d'une passerelle sans fil Z-Wave, vous ne devriez pas être rassurés. Il s'avère en effet que cette technologie – qui permet de contrôler des objets avec un rayon d'action de plusieurs dizaines de mètres – est vulnérable à une attaque par rétrocompatibilité baptisée « Z-Shave » permettant de prendre le contrôle de tous les appareils connectés à la même passerelle Z-Wave.
> Il suffirait d'être à proximité pour, par exemple, envoyer une commande d'ouverture à une serrure connectée et pénétrer dans l'habitation. Pour rappel, Z-Wave est une technologie maillée et décentralisée, largement utilisée dans les produits domotiques. L'usage de passerelles n'est pas obligatoire. Il permet, toutefois, d'ouvrir l'accès au réseau Z-Wave au monde extérieur (Internet).

Document 2 : *The Jeep Hackers Are Back to Prove Car Hacking Can Get Much Worse, Andy Greenberg, WIRED, 08/01/2016*[2] *(traduction de Louis Paternault).*

> Il y a presque exactement un an, Chrysler a rappelé 1,4 millions de véhicules après que deux *hackers* aient montré à WIRED qu'ils pouvaient prendre le contrôle du système informatique de la Jeep à distance, par internet.
> […]
> L'an passé, [les chercheurs en cybersécurité Valasek et Miller] ont pris le contrôle d'une voiture à distance, et l'ont arrêtée sur la route nationale I-64 — pendant que je la conduisais. […] Ils sont maintenant capables de réussir des tours encore plus inédits et dangereux, comme provoquer des accélérations non prévues, écraser les freins ou tourner le volant à n'importe quelle vitesse. « Imaginez que l'an passé, au lieu de couper la transmission sur la nationale, nous ayons tourné le volant à 180 degrés » demande Chris Valasek. J'imagine bien. Mais il précise quand même : « Vous ne seriez pas au téléphone avec nous en ce moment. Vous seriez mort. »
> […]
> Et ne vous trompez pas, disent les *hackers* de voiture : d'autres méthodes sans fil d'attaque de voitures seront trouvée, tôt ou tard.

1 https://www.01net.com/actualites/le-protocole-z-wave-met-votre-maison-connectee-a-la-portee-des-pirates-1457870.html

2 https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/

« Il y aura presque certainement d'autres vulnérabilités à distance dans le futur », dit Karl Koscher, un chercheur à l'université de Californie, à San Diego [...].
Comme ces scientifiques, Miller et Valasek ne cherchent pas à créer de chaos sur la route, mais à aider à créer de meilleurs protections avant que les attaques informatiques contre les voitures ne deviennent une vraie menace. [...] Les fabricants de voiture devraient aussi considérer que les pirates informatique finiront par trouver une brèche à distance, et construire des systèmes qui réduisent les conséquences désastreuses de telles failles. « Il faut savoir ce que les pirates vont faire ensuite, comment s'en protéger, et que certaines protections ne fonctionneront pas, comme nous l'avons montré » dit Miller.
Dans un article qui devrait être publié au moment de leur conférence *Black Hat*, Miller et Valasek recommandent aux constructeurs d'aller plus loin pour éviter le genre de manipulations qu'ils ont mises en évidence. Par exemple, ils suggèrent que les constructeurs n'autorisent pas certains tests potentiellement dangereux à moins qu'un interrupteur physique ne soit actionné par le garagiste.

Objets connectés et Sécurité

Après avoir brièvement résumé le premier document, vous expliquerez comment des objets connectés non sécurisés peuvent être une menace pour d'autres personnes, sans que les propriétaires de l'objet n'en soient conscients.

Document 1 : *Leaked Mirai Malware Boosts IoT Insecurity Threat Level, Douglas Bonderud, SecurityIntelligence.com, 4/10/2016*[1] *(traduction de Louis Paternault ; les mots marqués d'un astérisque* sont expliqués dans le document 2).*

Comme expliqué par le magazine *Infosecurity*, Mirai* est conçu pour tirer profit de l'IoT* en parcourant le web à la recherche d'appareils protégés par des mots de passe par défaut, ou par des identifiants codés en dur, les rendant facile à compromettre et à infecter. Une fois sous le contrôle de personnes mal intentionnées, ces appareils sont transformés en une sorte d'immense botnet* qui peut lancer des attaques par déni de service* sur des sites web, et les faire tomber rapidement.
Le site *Krebs on Security*, par exemple, a été récemment la cible d'une attaque par déni de service à 620 Gbps utilisant le logiciel malveillant Mirai. *Ars Technica* a aussi fait état d'une attaque à 1 Tbps visant l'hébergeur français OVH.
Dans les deux cas, ce trafic est d'un ordre de grandeur supérieur au nécessaire pour faire tomber un site web. Cela a été rendu possible par la combinaison du simple nombre d'appareils connectés à internet, et de la médiocre sécurité associée à la plupart de ces produits.
[…]
Selon *Ars Technica*, les caméras IP et les magnétoscopes numériques sont parmi les appareils connectés les plus souvent compromis. Cela se tient, car des millions de ces appareils sont en ligne, et la plupart sont livrées avec des identifiants de connexion qui ne sont jamais changés par la suite.
Le problème est que les caméras, les caméscopes, les imprimantes et les capteurs sans fil ne semblent pas dangereux parce qu'ils sont en périphérie des réseaux professionnels.
[…]
Comment donc les fabricants et les vendeurs d'objets connectés peuvent-ils inverser la tendance et stopper Mirai* dans sa course ? La première solution est les mots de passe. Les vendeurs d'appareils doivent s'assurer que chaque appareil connecté possède un mot de passe unique, ou forcer les utilisateurs à changer le mot de passe dés que l'appareil est installé.

Document 2 : *Extraits d'article de Wikipédia.*

Mirai : Mirai est un logiciel malveillant qui transforme des ordinateurs utilisant le système d'exploitation Linux en bots contrôlés à distance, formant alors un

1 https://securityintelligence.com/news/leaked-mirai-malware-boosts-iot-insecurity-threat-level/

botnet utilisé notamment pour réaliser des attaques à grande échelle sur les réseaux.

Attaque par dénie de service : Une attaque par déni de service [...] est une attaque informatique ayant pour but de rendre indisponible un service, d'empêcher les utilisateurs légitimes d'un service de l'utiliser.

IoT : L'Internet des objets, ou IdO (en anglais Internet of Things, ou IoT) est l'interconnexion entre Internet et des objets, des lieux et des environnements physiques.

Botnet : Un botnet [...] est un réseau de bots informatiques, des programmes connectés à Internet qui communiquent avec d'autres programmes similaires pour l'exécution de certaines tâches. [...] Le sens de botnet s'est étendu aux réseaux de machines zombies, utilisés notamment pour le minage de cryptomonnaies mais aussi des usages malveillants, comme l'envoi de spam et virus informatiques, ou les attaques informatiques par déni de service (DDoS).

Informatique embarquée et Morale

Après avoir brièvement résumé les documents ci-dessous, vous expliquerez quel problème moral peut poser une voiture autonome, et si une solution universelle à ce problème existe.

Document 1 : *Il n'y a pas de solution universelle au dilemme moral de la voiture autonome, Amy Maxmen, Nature, 24/10/2018[1] ; traduit par Philippe Ribeau, Pour la Science, 26/10/2018[2].*

Lorsqu'un conducteur appuie sur les freins pour éviter de heurter un piéton qui traverse la route, il prend sans s'en rendre compte une décision morale qui transfère le risque du piéton aux passagers de la voiture : vaut-il mieux renverser le piéton ou risquer de blesser les passagers ? Les voitures autonomes devront bientôt porter elles-mêmes de tels jugements éthiques – encodés dans leur logiciel de bord. Mais quel code moral doit-on implémenter dans les véhicules autonomes ? Une vaste enquête menée auprès de 2,3 millions de personnes dans le monde suggère qu'il pourrait être difficile de s'entendre sur un code éthique universel en la matière…

[…]

L'enquête, appelée la « Machine morale », présentait 13 scénarios dans lesquels la mort d'une personne était inévitable. Les participants devaient choisir qui épargner dans des situations qui impliquaient différentes combinaisons de variables : jeunes ou vieux, riches ou pauvres, homme ou femme, nombre de personnes impliquées, etc.

[…]

Quels enseignements se dégagent ? Premièrement, quel que soit leur âge, leur sexe ou leur pays, la plupart des gens préfèrent épargner les humains plutôt que les animaux de compagnie, et plutôt les groupes que les individus seuls. […]

Mais l'accord s'arrête là. Lorsque les auteurs ont analysé les réponses provenant des 130 pays ayant comptabilisé au moins 100 participants, ils ont constaté que les pays pouvaient être divisés en trois groupes. […] Les participants des pays du premier groupe montrent par exemple une plus grande préférence pour sacrifier les personnes âgées et sauver les jeunes que ceux des pays du second groupe.

Document 2 : *La voiture autonome et ses implications morales, Sandberg Anders et Bradshaw-Martin Heather, Multitudes, n°58, 2015 (traduction de Mona Gérardin-Laverge)[3].*

1 https://www.nature.com/articles/d41586-018-07135-0

2 https://www.pourlascience.fr/sd/science-societe/il-ny-a-pas-de-solution-universelle-au-dilemme-moral-de-la-voiture-autonome-15004.php

3 http://www.multitudes.net/la-voiture-autonome-et-ses-implications-morales/

Dans [des] circonstances tragiques, comment considérerions-nous le comportement d'un véhicule autonome ?
[…]
Une troisième possibilité serait d'exiger que l'usager du véhicule choisisse, avant d'utiliser le véhicule, ce qu'il voudrait que le véhicule fasse dans de telles circonstances. Dans ce cas, si le véhicule agit conformément au choix de l'usager, et si le véhicule interprète correctement le choix sélectionné, les fabricants et les ingénieurs n'auront pas à se justifier de son comportement. La responsabilité morale revient alors à celui à qui elle incombe actuellement – à celui qui utilise le véhicule à ce moment-là.