Roman LATTE

Les objets connectés, IOT (Internet Of Things) : leur exploitation dans le cadre d'une enquête judiciaire

Promotion 2024-2025

L'omniprésence croissante des Objets Connectés (IoT pour Internet Of Things, Internet des Objets Connectés) dans notre quotidien, des dispositifs portables aux systèmes domotiques et véhicules intelligents, génère une quantité massive de données numériques. Cette explosion de données représente une source d'information inestimable, mais complexe, pour les enquêtes judiciaires. Cet article explore le potentiel des données issu des objets connectés comme preuves numériques et analyse les défis inhérents à leur exploitation en contexte forensique. Nous examinerons la typologie des objets connectés pertinents, les types de données qu'ils génèrent et leurs apports significatifs dans la reconstitution des faits et l'identification des acteurs. Parallèlement, nous discuterons des défis techniques tels que la volatilité et le chiffrement des données, ainsi que des enjeux juridiques et éthiques majeurs relatifs à la protection de la vie privée et à l'obtention des autorisations nécessaires pour l'enquête judiciaire. Nous détaillerons également les méthodologies et outils de criminalistique numérique spécifiques aux objets connectés, soulignant l'importance d'une chaîne de garde rigoureuse et de compétences spécialisées. En conclusion, nous mettrons en lumière les perspectives d'évolution et les recommandations pour adapter les cadres légaux et les pratiques d'investigations face à la dynamique rapide de l'IoT, afin de maximiser leur contribution à l'administration de la justice.

1. Introduction

L'avènement des objets connectés a profondément transformé notre environnement quotidien, intégrant des millions, bientôt des milliards, de dispositifs connectés dans nos vies personnelles et professionnelles. Des montres intelligentes qui surveillent notre activité physique aux systèmes domotiques qui gèrent nos foyers, en passant par les véhicules autonomes et les infrastructures urbaines intelligentes, ces objets génèrent une quantité exponentielle de données. Ces données, souvent capturées en temps réel et stockées localement ou dans le cloud, décrivent nos habitudes, nos déplacements, nos interactions et même nos états physiques et physiologiques, créant ainsi une empreinte numérique de nos vies.

Cette prolifération technologique, tout en offrant des avantages considérables en termes de confort, d'efficacité et de personnalisation, soulève également des questions fondamentales, notamment dans le domaine de la justice. Les données issues des objets connectés peuvent devenir des preuves numériques capitales, capables de reconstituer des scènes de crime, de localiser des suspects ou des victimes, d'établir des chronologies précises, voire de révéler des intentions. Leur potentiel à éclairer des zones d'ombre dans des enquêtes complexes est indéniable, offrant aux enquêteurs des pistes d'investigations inédites et des éléments de preuve potentiellement irréfutables.

Cependant, l'exploitation de ces sources d'informations par les forces de l'ordre et les experts judiciaires n'est pas sans défis. La diversité des technologies IoT, l'hétérogénéité des formats de données, la volatilité de certaines informations et la complexité des infrastructures de stockage (locales ou cloud) constituent des obstacles techniques majeurs. À cela s'ajoutent des enjeux juridiques et éthiques de taille, notamment la protection de la vie privée, la conformité avec des régulations strictes comme le Règlement Général sur la Protection des Données (RGPD), la nécessité d'obtenir des ordonnances judiciaires ou autorisations spécifiques, et la question de la localisation des données. La force probante de ces éléments numériques, leur intégrité et leur authenticité, doivent également être garanties pour qu'ils soient admissibles et convaincants devant un tribunal.

Le présent article vise à analyser en profondeur l'intérêt et l'apport des objets connectés dans le cadre des enquêtes judiciaires, tout en identifiant et en discutant les défis majeurs que leur exploitation soulève. Nous explorerons les différentes catégories d’objets connectés pertinentes pour l'investigation numérique, les types de données qu'elles génèrent et leur potentiel. Nous détaillerons ensuite les obstacles techniques, juridiques et éthiques rencontrés par les enquêteurs et les experts en criminalistique numérique. Enfin, nous présenterons les méthodologies et les outils actuellement mis en œuvre, ainsi que les perspectives d'évolution pour adapter le cadre légal et les pratiques d'investigations face à la dynamique rapide des objets connectés, contribuant ainsi à une meilleure compréhension de ce domaine en pleine mutation.

2. L'Internet des Objets (IoT) : Définition, Types et Données Générées

Pour comprendre l'impact des objets connectés sur les enquêtes judiciaires, il est essentiel de les définir et de catégoriser les types d'appareils et de données qu'ils englobent.

Concernant la définition :

L'IoT a une évolution exponentielle, équipé de capteurs, de logiciels et d'autres technologies, permettant de se connecter et d'échanger des données avec d'autres appareils et systèmes sur Internet ou d'autres réseaux de communication. La définition même de l'IoT réside dans sa capacité à "parler" entre eux, à collecter des informations sur leur environnement ou sur leurs utilisateurs, et de les transmettre pour analyse ou action dans des logiciels par exemple.

En définitive, l'IoT, c'est quand des objets du quotidien sont connectés à Internet pour échanger des informations et agir automatiquement sans une intervention humaine, comme par exemple une montre connectée qui mesure un rythme cardiaque et le transfère les données sur un téléphone pour, par la suite, te donner des conseils pour faire baisser le rythme.

Concernant les différentes sortes d'objets :

La diversité des objets connectés signifie que chacun peut potentiellement fournir des types de données uniques. Pour les enquêteurs, il apparaît important de savoir quels sont les objets à rechercher et quels types d'informations, ces objets sont susceptibles de contenir.

- **Les objets « Portables » :**
  Il s'agit par exemple, des montres connectées, intelligentes (Apple Watch, Garmin), les bracelets de fitness (Fitbit), ou même certains vêtements connectés, sont en contact direct et constant avec l'utilisateur et son téléphone. Avec ces objets, les données suivantes peuvent nous être fourni, telles que : la fréquence cardiaque, le nombre de pas, la qualité du sommeil, la position GPS (parfois), l'historique des notifications, et des données d'activité physique. Ces informations peuvent établir une chronologie précises des mouvements, le niveau d'activité ou même l'état physiologique d'une personne à un moment précis.

- **Les objets de la maison « intelligente » :**
  De plus en plus courants, ces dispositifs transforment le domicile en une source d'informations numériques, notamment :

→ Les enceintes connectées chez Amazon, Google et Microsoft par exemple. Ces appareils, enregistrent et analysent les commandes vocales. Ces enceintes collectent entre autres des données sur la présence humaine (mouvements détectés), les habitudes de chauffage/refroidissement, et parfois l'humidité. Elles peuvent enregistrer des vidéos et des sons (caméras de vidéos surveillance, interphone), détectent les mouvements, et peuvent stocker ces enregistrements localement ou sur le cloud. Elles sont inestimables pour prouver la présence, identifier des individus ou des véhicules.

→ Les serrures connectées. Elles enregistrent les accès (qui est entré et quand), et peuvent être une preuve directe d'intrusion ou de présence autorisée.

→ Les véhicules connectés. Les automobiles modernes sont de véritables ordinateurs roulants, équipés de multiples capteurs et systèmes connectés. Les données générées sont une mine d'information, notamment concernant la localisation GPS, l'historique des trajets, la vitesse, les connexions Bluetooth (à quels téléphones l'appareil a été associé). Ces informations sont cruciales pour reconstituer un itinéraire, déterminer la responsabilité dans un accident ou même identifier des passagers.

→ Les appareils médicaux connectés. Comme les pacemakers, les pompes à insuline intelligente, les moniteurs de glycémie. Les données générées peuvent fournir des indications sur l'état physiologique d'une personne et l'administration de médicaments. Bien que très sensibles, ces données peuvent être vitales dans des enquêtes impliquant la santé d'une personne ou des incidents médicaux.

Concernant le type de données et le stockage de celles-ci :

La diversité des appareils existants, se traduit par une variété tout aussi grande de types de données. Pour les enquêteurs, comprendre et comment les données des objets connectés sont stockés est devenu fondamental et nécessaire.

→ **Données de localisation :**

GPS, Wi-Fi, Bluetooth (avec les appareils connectés à proximité), géolocalisation des téléphones. Ces données sont essentielles pour établir la présence d'une personne ou d'un objet à un endroit donné sur une scène d'infraction.

→ Données biométriques et de santé :

Fréquence cardiaque, sommeil, nombre de pas, calories brûlées…. Ces données fournissent des informations essentielles sur l'état physique et l'activité d'un individu. Cela peut permettre de savoir si un individu a eu un pic d'activité à un instant T, permettant d'obtenir l'un des faisceaux d'indices sur la personne soupçonnée.

→ Données d'activité et d'utilisation :

L'historique de navigation web, nous permet par exemple de comprendre si l'auteur d'une infraction a potentiellement prémédité son geste en effectuant des recherches.

→ Contenus multimédias :

→ Le contenu des images et vidéos de caméras de sécurités, les enregistrements audio de certaines enceintes connectées. Ces données, notamment pour les caméras de vidéos surveillances permettent d'obtenir des preuves directes et souvent très impactantes pour la suite de l'enquête.

Concernant le stockage des données :

Pour les nécessités de l'enquête, il est important de connaître le lieu précis de **stockage** des données afin de ne pas faire d'erreur de procédure. Cette identification de « stockage des données » est un facteur clé de l'enquête judiciaire et il peut être de différentes sortes, notamment :

- **Localement sur l'appareil :** Les données peuvent être stockées directement sur la mémoire interne de l'objet, par exemple, un enregistrement vidéo sur une carte SD d'une caméra. L'accès direct à l'appareil est alors primordial.
- **Sur un appareil associé :** Souvent, l'IOT est lié à un smartphone ou une tablette via une application mobile. Les données sont alors synchronisées et peuvent résider l'IOT mais également sur le téléphone.
- **Dans le Cloud :** Une grande partie des données IOT est transmise et stockée sur les serveurs des fabricants ou des fournisseurs de services (Amazon Apple, Google, Microsoft etc.). C'est le cas pour la plupart des enregistrements de caméras de sécurité. L'accès à ces données nécessite des requêtes légales auprès de tiers, ce qui introduit des complexités au sein de l'enquête, notamment des complexités juridictionnelles et de délais.

Il faut bien comprendre cette typologie et ces modes de stockage ; En effet, il s'agit de la première étape pour les enquêteurs, qui doivent savoir où chercher la preuve numérique et comment y accéder de manière légale et technique. C'est justement l'intérêt de ces données pour les enquêtes que nous allons aborder.

3. Intérêt et Apports de l'IOT dans l'Enquête Judiciaire

L'intégration croissante des objets connectés dans nos vies a ouvert de nouvelles frontières pour la criminalistique numérique, offrant aux enquêteurs des sources de preuves inédites et souvent déterminantes. Les données issues de ces dispositifs peuvent enrichir considérablement une enquête, allant de la simple confirmation d'un alibi à la reconstitution complexe d'une scène de crime.

Au cœur de l'apport des IOT réside leur capacité à générer des preuves numériques formelles et horodatées. Contrairement aux témoignages humains qui peuvent être sujets à l'erreur ou à la manipulation, les données des objets connectées sont souvent des enregistrements factuels d'événements. Elles permettent d'établir des éléments matériels qui peuvent corroborer ou contredire des déclarations, et ainsi renforcer la crédibilité d'une affaire. Par exemple, les enregistrements d'une caméra de sécurité peuvent fournir des preuves directes de la présence d'une personne, d'un véhicule ou de la survenue d'un événement à un moment précis.

<u>L'une des contributions les plus significatives de l'IOT est sa capacité :</u>

→ A aider à la reconstitution des faits, notamment avec la localisation et les déplacements, Les données GPS des véhicules connectés, les informations de géolocalisation des montres intelligentes peuvent cartographier les déplacements d'un objet. Elles permettent de prouver une présence sur les lieux d'un crime ou, au contraire, d'établir un alibi solide.

→ A établir l'emploi du temps d'une personne notamment avec la chronologie des évènements, à connaître son mode de vie . Il s'agit de l'état d'activité d'une personne. Chaque donnée IOT est généralement horodatée. En recoupant les journaux d'activité de plusieurs appareils (une serrure connectée ouverte à une certaine heure, des lumières intelligentes allumées, des pas détectés par un bracelet d'activité), les enquêteurs peuvent construire une chronologie détaillée des événements, souvent minute par minute. Cela est crucial pour comprendre le déroulement exact d'un incident. Par exemple, savoir quand une porte de maison connectée a été ouverte peut s'avérer vital.

→ A connaître ses relations familiales, amicales ou amoureuses. Avec l'analyse du contenu des objets tel un téléphone. Il est possible de connaître les principaux contacts, les principales relations….

Les objets connectés peuvent également aider à l'identification des personnes impliquées dans une affaire. En effet, les journaux de connexion Bluetooth d'un véhicule peuvent révéler quels téléphones ont été jumelés, et donc qui était potentiellement à bord. Les enceintes connectées et les caméras de sécurité peuvent parfois être équipées de fonctions de reconnaissance vocale ou faciale, permettant d'identifier des voix ou des visages spécifiques, même si ces technologies posent des défis en termes de fiabilité et de vie privée. Les historiques d'utilisation des applications associées aux IOT sur un smartphone peuvent montrer quand et comment un utilisateur a interagi avec ses objets connectés, fournissant des indices sur ses intentions ou ses actions.

Nous allons aborder quelques cas concrets, ou plusieurs affaires emblématiques ont déjà démontré l'impact de l'IOT sur les enquêtes judiciaires, notamment outre-atlantique.

→ Le cas de la montre Fitbit dans l'affaire Connie Dabate (États-Unis) :

En 2015, les données d'une montre Fitbit ont été utilisées pour contredire le témoignage d'un mari accusé du meurtre de sa femme. La montre a montré que la victime était en mouvement et vivante au moment où l'accusé prétendait qu'elle avait déjà été tuée, permettant d'établir une chronologie des faits incompatible avec la version de l'auteur.

→ L'affaire de l'enceinte Amazon Alexa (États-Unis), meurtre de Victor Collins :

En 2016, dans une affaire de meurtre en Arkansas, la police a cherché à obtenir les enregistrements audio d'une enceinte Amazon Alexa appartenant au suspect. Bien que l'accès initial ait été refusé par Amazon au nom de la vie privée, le suspect a finalement autorisé lui-même la divulgation des données, qui contenaient potentiellement des informations cruciales sur les événements de la nuit du crime. Ce cas a mis en lumière la tension entre vie privée et impératifs d'enquête.

→ Les véhicules connectés en cas d'accident :

De nombreux véhicules modernes enregistrent des données sur la vitesse, le freinage, l'accélération et même les impacts. Ces "boîtes noires" peuvent être extraites et analysées pour reconstituer la chronologie d'un accident, de déterminer les responsabilités et vérifier les déclarations des conducteurs.

Ces exemples illustrent la valeur probante des données IOT, transformant des objets du quotidien en témoins « silencieux », « discrets » capables de fournir des éléments essentiels à la manifestation de la vérité. Cependant, cette richesse de l'information s'accompagne d'un ensemble complexe de défis techniques, juridiques et éthiques que nous allons explorer.

4. Les défis majeurs de l'exploitation des données des objets connectés

Si l'apport des objets connectés est indéniable, leur exploitation en contexte judiciaire est semée d'embûches. Les enquêteurs et les experts en criminalistique numérique doivent naviguer à travers un labyrinthe de complexités techniques, juridiques et éthiques qui peuvent compromettre la collecte des données, l'analyse et l'admissibilité des preuves.

La nature hétérogène et dynamique des objets connectés présente une série de difficultés techniques pour diverses raisons.

→ Les données disparaissent vite. Nous parlons de volatilité des preuves. Beaucoup de données des objets connectés ne restent pas indéfiniment. Elles peuvent être écrasées, effacées automatiquement (pour gagner de la place ou à cause des règles de confidentialité du fabricant), ou simplement jamais enregistrées sur l'appareil. Par exemple, la durée de conservation des enregistrements de caméras de sécurité. Perdre rapidement ces informations vitales est un risque constant si l'enquête n'agit pas tout de suite.

→ Il existe une multitude d'appareils différents et des systèmes variés. En effet, l'univers des objets connectés est un mélange de marques, de systèmes d'exploitation, de formats de données et de façons de communiquer, souvent propres à chaque fabricant. Contrairement aux ordinateurs ou téléphones qui ont des normes, il n'y a pas de méthode unique pour récupérer les données d'un objet connecté. Chaque appareil peut demander des outils, des techniques ou des connaissances spécifiques, ce qui complique la tâche et allonge énormément le délai d’enquête et le travail des enquêteurs.

→ Il existe des données de formats différents et difficiles à comprendre. Même quand nous arrivons à récupérer les données, celles-ci peuvent être dans des formats non standards, souvent impossibles à lire sans les logiciels ou les clés de déchiffrement adéquats. Comprendre les données brutes demande une grande expertise, une grande technicité et de connaître les détails techniques du fabricant. Une simple date et heure peuvent ne pas être dans le bon fuseau horaire, ou une donnée de localisation peut être imprécise.

→ Dans le cadre d’une enquête judiciaire, il est important de garantir l'originalité des preuves. En effet, il est fondamental de s'assurer que les données récupérées soient originales, non modifiées par l’enquêteur ou au moment de la récupération, et authentiques pour qu'elles soient acceptées en justice. Les méthodes de récupération doivent respecter un protocole bien défini et pouvoir être refaites à l'identique. La fragilité de certains supports de stockage des objets connectés peut aussi rendre la récupération sans altération très délicate et difficile.

→ Garder une trace parfaite de toutes les preuves numériques venant des objets connectés est un défi majeur. Chaque étape, depuis l'identification de l'objet sur le lieu du crime jusqu'à son transport, sa conservation, son analyse et sa présentation au tribunal, doit être documentée avec précision pour s'assurer que rien n'a été modifié et que tout est traçable. Une erreur dans cette chaîne peut rendre la preuve inutilisable, et tout ce qui en découle deviendrait caduc.

→ Le dernier point concernant les difficultés techniques, la compétence des enquêteurs et des experts. En effet, l'évolution rapide des objets connectés exige que les enquêteurs numériques « cyber » mettent constamment à jour leurs connaissances. La formation continue est essentielle pour maîtriser les nouvelles technologies, les outils de récupération et les méthodes d'analyse spécifiques à ces appareils.

Au-delà des aspects techniques, l'exploitation des données objets connectés se heurte à des questions complexes de droit et d'éthique. La limite entre la nécessité d’obtenir des informations sur la personne, son mode de vie, sa localisation par exemple et sa vie privée et la protection de ses données personnelles. Plusieurs cas se présentent notamment sur la vie privée et protection des données personnelles. L’objet connecté collecte des données souvent très intimes (santé, localisation, habitudes de vie...) sur les individus. Le droit à la vie privée est un droit fondamental, et des réglementations comme le Règlement Général sur la Protection des Données (RGPD) en Europe imposent des conditions strictes pour la collecte, le traitement et le stockage des données personnelles. L'accès à ces données pour les besoins d'une enquête doit être strictement proportionné, encadré et légalement justifié.

De ce fait, l'accès aux données des objets connectés, surtout celles stockées sur des serveurs cloud (par exemple, chez Amazon, Google, Apple), nécessite généralement des autorisations (ou appelé commission rogatoire ou commission rogatoire internationale en France) de perquisition numérique ou des réquisitions judiciaires spécifiques. Obtenir ces autorisations peut être un processus long et complexe.

Ce qui pose une difficulté majeure lorsque les données sont stockées sur des serveurs situés dans un autre pays. Les lois du pays où sont stockées les données s'appliquent, et les procédures de coopération judiciaire internationale (demandes d'entraide judiciaire) sont notoirement lentes et complexes, entravant la rapidité de l'enquête.

N'oublions pas également que pour qu'une donnée issue d'un objet connecté soit admise comme preuve devant un tribunal, elle doit non seulement être pertinente et fiable, mais aussi respecter les règles de procédure pénale. La méthode de collecte et d'analyse doit être rigoureuse et pouvoir être démontrée lors d'un jugement. Les avocats de la défense peuvent contester l'authenticité, l'intégrité, l'interprétation ou même la légalité de la collecte de ces preuves, ce qui peut mettre à mal l'enquête judiciaire.

Dernier point important, non des moindres, la question du consentement de l'utilisateur à la collecte de ses données par l'IOT, et son droit potentiel à les faire supprimer (droit à l'oubli), complique l'accès à certaines informations, surtout si l'enquête survient longtemps après les faits.

Nous venons de voir que ces défis soulignent la nécessité d'une approche multidisciplinaire et d'une évolution constante du cadre législatif, des outils technologiques et des compétences humaines pour exploiter efficacement et légalement le potentiel des objets connectés. Nous allons aborder les différentes méthodologies et les outils d'investigations numériques.

5. Méthodologies et outils d'investigation numérique pour l'objet connecté

Concernant la méthodologie :

Face à la complexité des défis techniques et juridiques, la criminalistique numérique de l'objet connecté s'est développée en adaptant les principes fondamentaux de l'investigation numérique aux spécificités des objets connectés. L'objectif est d'assurer une collecte, une analyse et une présentation des preuves qui soient à la fois complètes, fiables et admissibles en justice.

Le processus d'investigation numérique des objets connectés suit généralement des phases bien définies, inspirées des modèles forensiques classiques, mais avec des adaptations importantes.

Avant toute analyse, première phase, il faut ***identifier l'objet connecté***. Cette phase initiale consiste à déterminer quels objets connectés sont présents sur une scène de d'infraction ou pertinents pour l'enquête. Il s'agit de repérer les appareils susceptibles de contenir des données utiles (montres, enceintes, systèmes de sécurité domestique, véhicules, etc.) et de comprendre leur rôle potentiel dans les événements. Il est essentiel de ne rien négliger, car même un appareil apparemment anodin peut contenir des informations clés.

Dans un second temps, il faut ***protéger les données***. En effet, une fois identifiés, les objets connectés et leurs données doivent être préservés immédiatement pour éviter toute altération ou perte. C'est une étape critique étant donné la volatilité de nombreuses données liée aux objets connectés. Cela peut impliquer de déconnecter l'appareil du réseau (Wi-Fi, Bluetooth, cellulaire) pour éviter l'effacement à distance.

Puis, vient la phase de ***récupération des données ou « collecte »***. Cette phase consiste à extraire les données pertinentes de l'objet connecté ou de ses sources associées. Les techniques varient considérablement en fonction du type d'appareil et de l'endroit où les données sont stockées. Il faut soit faire :

→ Une copie complète de la mémoire. C'est la méthode la plus complète mais pas toujours possible pour tous les objets connectés.

→ Une copie de fichiers spécifiques : On extrait des fichiers ou des bases de données précises de l'appareil. C'est moins "invasif" mais peut-être moins complet.

→ Demander une copie des données aux différents services « Cloud » en effectuant des requêtes légales aux entreprises qui fournissent les services pour obtenir les données stockées sur leurs serveurs. Cela demande des autorisations particulières et est soumis aux lois internationales.

→ Analyser des applications présentes sur un smartphone. En effet, le smartphone ou la tablette connectée à l'objet contient souvent des données synchronisées ou l'historique des interactions avec l'objet. Analyser ces téléphones est donc un complément essentiel.

Avant-dernière phase concernant le processus d'investigation numérique des objets connectés, ***l'analyse***. Une fois les données brutes acquises, elles doivent être traitées, décodées, filtrées et interprétées. C'est l'étape où généralement « les experts » interviennent. L'analyse des données permet, entre autres, de reconstruire des chronologies et d'identifier des événements par exemple.

Dernière phase, ***la rédaction d'un rapport***. Cette dernière étape consiste à tout documenter. Du processus d'enquête, de la collecte à l'analyse, et à présenter les conclusions de manière claire, concise et scientifiquement irréprochable. Le rapport doit pouvoir être compris par des personnes qui ne sont pas des experts (juges, jurés) et doit être assez détaillé pour permettre une vérification par d'autres experts. Il doit aussi inclure un suivi complet de toutes les preuves numériques collectées.

Concernant les outils spécifiques :

Le marché de la criminalistique numérique a vu l'émergence d'outils spécialisés pour l'étude des objets connectés, en complément des suites logicielles traditionnelles. Ils ne sont pas tous listés car de nombreuses sociétés sont sur le marché, cependant les forces de l'ordre en France travaillent en collaboration avec des logiciels d'enquête numérique complets, tels que **Cellebrite, MSAB, AXIOM**….. Ces logiciels ont été améliorés pour inclure la récupération et l'analyse des données d'un nombre croissant d'appareils, comme les ordinateurs, téléphones, support de stockage.

Ils existent des outils spécifiques pour les véhicules connectés. Des plateformes américaines comme **Berla iVe** sont faites pour extraire, entre autres, les données des systèmes des "boîtes noires" des voitures, très importantes pour les enquêtes sur les accidents ou les vols de véhicules.

Ils existent également en **OSINT** (open source) de nombreux outils qui peuvent être utilisés pour accéder aux données. Cela demande des compétences techniques indispensables en "ingénierie " et en programmation.

L'efficacité d'une enquête sur un objet connecté vient souvent de la capacité à croiser les différentes informations provenant de plusieurs sources, l'appareil lui-même, l'application mobile associée sur un smartphone, les serveurs cloud du fabricant ou du fournisseur de services, et même les informations de localisation des opérateurs de téléphone. Ce faisceau d'indices de données permet de créer une image plus complète et plus solide de ce qui s'est passé afin de permettre une résolution d'enquête.

La complexité des investigations concernant les objets connectés rend la formation continue des enquêteurs et des experts absolument indispensable. Ils doivent non seulement maîtriser les aspects techniques de l'extraction et de l'analyse, mais aussi comprendre les implications juridiques et éthiques de leurs actions. De ce fait, la collaboration est essentielle. En effet, les forces de l'ordre doivent travailler en étroite synergie avec l'ensemble des acteurs tels que :

→ Les experts en criminalistique numérique (souvent des laboratoires spécialisés).

→ Les fournisseurs de services cloud et les fabricants d'objets connectés pour obtenir les données et des informations techniques sur leurs produits

→ Les légistes et magistrats pour s'assurer que les méthodes utilisées sont conformes au droit et que les preuves seront admissibles.

En intégrant ces méthodologies et en s'appuyant sur des outils spécialisés, les enquêteurs peuvent naviguer plus efficacement dans le paysage complexe des objets connectés, transformant leurs données en preuves numériques solides pour la justice. La section suivante explorera les perspectives et recommandations pour l'avenir de ce domaine en constante évolution.

6. Perspectives et Recommandations

L'objet connecté, avec son évolution rapide et son intégration de plus en plus profonde dans tous les aspects de nos vies, continuera d'offrir des opportunités sans précédent pour l'administration de la justice, mais aussi de poser des défis persistants. Pour que les enquêtes judiciaires puissent exploiter pleinement le potentiel des objets connectés, plusieurs perspectives et recommandations s'imposent.

L'objet connecté est en perpétuelle mutation. L'émergence de technologies comme la 5G, l'intelligence artificielle (IA) embarquée directement dans les appareils, modifiera la manière dont les données sont collectées, traitées et stockées.

Les enquêteurs devront anticiper ces changements, adapter leurs outils et leurs compétences pour faire face à ces nouvelles architectures de données et à ces nouveaux appareils. La veille technologique et la recherche proactive sur les objets connectés sont essentielles.

L'un des gros problèmes actuels est le manque de règles communes dans l'univers de l'objet connecté. Pour résoudre cela, certaines évolutions devraient être nécessaires dont :

→ L’uniformisation des données et les systèmes de communication. Il faudrait encourager les fabricants à utiliser des formats de données. Cela rendrait beaucoup plus facile la récupération et l'analyse des données par les outils d'enquête, en réduisant le temps et la complexité des analyses.

→ Le développer des méthodes d'extraction. Il faudrait créer et adopter des méthodes de récupération de données qui sont prouvées scientifiquement et reconnues partout pour les différentes catégories d'objets connectés. Cela garantirait que les preuves soient originales et authentiques, ce qui les rendrait plus solides devant les tribunaux.

→ Pour ce faire, il faudrait mieux travailler avec les fabricants. Une bonne coopération pour comprendre comment leurs systèmes de données fonctionnent, quelles sont leurs mesures de sécurité et, si possible, obtenir les outils ou les informations techniques nécessaires aux enquêtes, tout en respectant la confidentialité et la propriété intellectuelle.

Le droit a souvent du mal à suivre le rythme des nouvelles technologies. Il est crucial d'adapter les lois de manière proactive. Les lois existantes doivent être revues et rendues plus claires pour encadrer spécifiquement l'accès, la collecte et l'utilisation des données des objets connectés. Il faut trouver un juste équilibre entre les besoins de l'enquête et les droits fondamentaux à la vie privée. Le renforcement de la coopération entre pays pour faire face à la complexité des données stockées dans différents pays (souvent dans le "cloud" à l'étranger), il faut des mécanismes de coopération judiciaire internationale plus rapides et efficaces. Des accords entre pays, pourraient faciliter l'accès légal aux preuves qui se trouvent au-delà des frontières. Dernier point concernant le droit, la sensibilisation et la formation des « acteurs » de la justice. Les juges, procureurs et avocats doivent être mieux formés aux aspects techniques et légaux des objets connectés pour comprendre la valeur et les limites des preuves numériques, ainsi que les implications éthiques de leur utilisation.

7. Conclusion

Les objets connectés font maintenant partie de notre quotidien et ont changé la façon dont les enquêtes se déroulent. Ils offrent aux professionnels des outils puissants pour reconstituer les faits et identifier les personnes. Les données qu'ils génèrent, qu'elles viennent de montres intelligentes, de systèmes de maison connectée ou de voitures, sont des preuves numériques concrètes. Elles peuvent aider à comprendre des situations complexes et à rendre les conclusions des enquêtes plus solides.

Cependant, cette opportunité s'accompagne de gros défis. Les problèmes techniques, liés à la variété et à la façon dont les données sont stockées ou cachées, demandent des compétences spéciales et des outils adaptés. En même temps, les questions légales et éthiques, comme la protection de la vie privée, l'obtention des autorisations nécessaires et le problème des données à l'étranger, demandent une attention constante et des adaptations de la loi.

Pour que les objets connectés puissent vraiment aider la justice, il est essentiel d'agir de manière proactive. Cela veut dire mettre en place des normes communes, adapter constamment les lois pour trouver le bon équilibre entre les besoins de l'enquête et nos droits fondamentaux, renforcer la collaboration internationale, et investir beaucoup dans la formation et la recherche.

Malgré leur complexité, les objets connectés sont devenus des témoins silencieux et omniprésents de nos vies. Les maîtriser pour les enquêtes n'est pas seulement une question de progrès technologique, mais une nécessité pour s'assurer que la justice puisse s'adapter à la réalité numérique de notre époque, garantissant ainsi l'équité et la pertinence de ses décisions.

Références Bibliographiques

- La criminalistique numérique appliquée à l'IoT, avec un article intitulé « L'internet des objets connectés à l'épreuve de la criminalistique numérique » publiée dans la revue de la Gendarmerie Nationale (n°268)
- Thèse de M. BOUCHAUD François intitulée « Analyse forensique des écosystèmes intelligents communicants de l'internet des objets » rédigé entre 2016 et 2020
- Une étude internationale retrouvée en archive ouverte sur ArXiv en 2018 nommée « Internet of things forensic : Challenges and Case Study » qui détaille les problématiques de collecte des données issues des objets connectés.
- Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et de la libre circulation de ces données. RGPD (Règlement Général sur la Protection des Données