Utilisation des objets connectés en EPS

***Aspects juridiques** liés à l'utilisation des données personnelles recueillies*

Les objets connectés, qu'est ce que c'est ?

Ce sont les appareils **contrôlables à distance** soit via le web soit via des applications dédiées et qui **transmettent des données** à leurs propriétaires et peuvent même interagir avec lui (enceinte, montres, cardio-fréquencemètre, smartphones, tablettes, cordes à sauter, drones, télévision, ordinateur, …). Ces appareils peuvent aussi **partager des données d'usages avec les fabricants** sous prétexte de les rendre plus intelligents. Ces échanges posent la question de la confidentialité des données transmises.

En tant qu'enseignant **nous devons assurer la protection** des données personnelles des élèves afin d'éviter leurs récupérations à des fins non connues.

Quelles données peuvent être récupérées ?

Les données personnelles au sens du **RGPD** (Règlement Général pour la Protection des Données) sont toutes les données permettant **d'identifier un individu directement ou indirectement** : nom, adresse postale ou électronique, numéro de sécurité, historique des données de navigation web, adresse IP, photos, données de géolocalisation, numéro carte de paiement, plaque d'immatriculation, photos, avatar, …

Leurs divulgations ou leurs mauvaises utilisations **pourraient porter atteinte** aux droits et libertés des personnes ou à leur vie privée. En croisant au moins deux données, on obtient des informations. Ces **informations peuvent être revendues** à d'autres exploitants (cf. les CGU des matériels et des applications) et après analyses, donner des renseignements sur la vie privée des usagers et donc des élèves (mode de vie d'une classe d'âge, état de santé global des jeunes, …).

Un appareil connecté perd souvent en sécurité lorsqu'il gagne en mobilité. La sécurité et la protection des données personnelles sont indéniablement des défis majeurs à leur diffusion et **la problématique de la confidentialité doit être maîtrisée**.

Que dit le RGPD ?

A compter du 25 mai 2018, Le RGPD impose aux entreprises (et aussi aux établissement scolaires) qui traitent et hébergent des données personnelles de **nouvelles obligations strictes** (tenue d'un registre des traitements, étude d'impact des traitements présentant des risques, politique de recueil des consentements, notification des failles de sécurité, nouveaux droits protégeant les données personnelles).

Avec le RGPD les organisations sont donc maintenant **responsables des données qu'elles traitent**. Or les **données à caractère personnel** (DCP) des élèves manipulées par un établissement scolaire sont très nombreuses : état civil, groupe classe, enseignants, notes, connexions internet, livret scolaire, parcours scolaire, …

Les responsables de traitement de données (IA-DASEN pour les établissements du 1er degré, chef d'établissement pour les établissements du 2nd degré) sont responsabilisés : ils doivent documenter tous les traitements de données

à caractère personnel dans le registre du **délégué à la protection des données** (DPD).

<u>Le RGPD renforce les droits de personnes et en facilite l'exercice :</u>

L'expression du consentement doit être définie : les utilisateurs doivent être informés de l'usage de leurs données et doivent en principe donner leur accord pour le traitement de leurs données, ou pouvoir s'y opposer (***droit à la transparence***).

Les utilisateurs ont ***droit à la portabilité des données*** : ce nouveau droit permet à une personne de récupérer les données qu'elle a fournies sous une forme aisément réutilisable, et, le cas échéant, de les transférer ensuite à un tiers afin de redevenir maitre de leurs données. **Des conditions particulières pour le traitement des données des enfants** : l'information sur les traitements de données les concernant doit être rédigée en des termes clairs et simples, que l'enfant peut aisément comprendre. Le consentement doit être recueilli auprès du titulaire de l'autorité parentale.

Les utilisateurs ont le ***droit à l'oubli***, c'est à dire le droit à l'effacement des données personnelles qui les concernent.

Une clé de lecture : **la protection des données dès la conception** (*privacy by design*). Les responsables de traitements devront mettre en œuvre toutes les mesures techniques et organisationnelles nécessaires au respect de la protection des données personnelles, à la fois dès la conception du produit ou du service et par défaut.

La protection des données par défaut (*privacy by default***)**. Il s'agit de limiter la quantité de données personnelles traitées, leur accessibilité et leur durée de conservation : seules les données personnelles nécessaires au fonctionnement, pour ne garder que le strict nécessaire en fonction de la finalité du traitement. Concrètement, ils devront veiller à limiter la quantité de données traitée dès le départ (**principe dit de « minimisation »**).

Un allègement des formalités administratives et une **responsabilisation des acteurs**. Afin d'assurer une protection optimale des données personnelles qu'ils traitent de manière continue, les responsables de traitements et les sous-traitants devront mettre en place des **mesures de protection des données** appropriées et démontrer cette conformité à tout moment (principe d'«***accountability»***).

De nouveaux outils de conformité :

- la tenue d'un registre des traitements mis en œuvre
- la notification de failles de sécurité (aux autorités et personnes concernées)
- la certification de traitements
- l'adhésion à des codes de conduites
- les études d'impact sur la vie privée (EIVP)
- nommer un DPD délégué à la protection des données (ou DPO)

Le rôle du DPD sera de sécuriser et clarifier la gouvernance des données que l'entreprise manipule et vérifier leur conformité afin de restaurer un climat de confiance entre entreprises et utilisateurs.

D'autres informations sur le RGPD ici :
https://www.cnil.fr/fr/reglement-europeen-sur-la-protection-des-donnees-ce-qui-change-pour-les-professionnels

https://dane.ac-lyon.fr/spip/FAQ-RGPD-Reglement-General-pour-la

Quels objets connectés possibles en EPS et quels types de récupération des données possibles ?

Outre l'adresse mail (ainsi que les noms et prénoms des utilisateurs), quasiment toujours nécessaire à la création d'un compte pour pouvoir utiliser un objet connecté ou une application, d'autres types de données peuvent être récupérées et présenter différents risques potentiels.

Objets connectés	Quels types de récupérations des données possibles et quels risques potentiels ?
Enceinte	Récupérer les types de musiques jouées pour en proposer d'autres avec des playlists qui ne sont pas toujours adaptées (paroles vulgaires, clips vidéo avec des images inadaptées, des publicités inappropriés, …)
Montres	Récupérer des données santé (pouls, calories, informations personnelles sur son état de santé, pratique physique, trace GPS, appels passés, sms reçus, …). On peut en déduire l'activité physique d'une personne, son état de santé global, les trajets réalisés ainsi que leurs horaires, les appels réalisés, …
Cardio-fréquencemètre	Récupération de l'évolution de la fréquence cardiaque au regard de l'effort produit, ainsi que d'autres données qui peuvent informer sur l'état de santé.
Smartphones	Tout peut être récupérable par les différentes applications. Le croisement de ces données donne des informations très précises sur la vie privée des personnes. Messages publiés, photos diffusées (ou stockées sur des cloud), âge, sexe, mode de vie, adresse, déplacements, …
Tablettes	Identique au smartphone sauf si l'appareil n'est pas connecté à un réseau wifi ou 4G (données seulement dans la tablette). Toutefois à la moindre connexion, les applications peuvent transmettre les données collectées.
Corde à sauter	Calories dépensées, accès aux données santé, …
Ordinateur	Contient bien souvent toutes les informations importantes sur la vie des personnes. En analysant les sites internet visités, votre adresse, vos papiers transmis par mail, vos codes, … on peut savoir exactement ce que vous faites !

Comment prévenir ces risques potentiels ?

En résumé, pour éviter que toutes les données recueillies ne soient directement associées à une personne désignée, nous devons garantir l'anonymat de nos élèves (bien souvent mineurs).
Pour cela nous pouvons préconiser les actions suivantes :

- Éviter que deux informations « vraies » puissent être croisées par une application.
- Anonymer au maximum toutes les informations transmises par les objets connectés : indiquer des pseudonymes ou ne mettre que le prénom pour séparer l'identité élève des données collectées.
- Limiter au maximum les informations transmises si elles ne sont pas essentielles au fonctionnement de l'objet ou de l'application ou en indiquer des « standards » qui ne permettent pas de reconnaître une personne.
- Lire les CGU (cocher, décocher) des applications installées et utilisées sur les différents supports. N'installer que les applications dont la transparence est évidente et la sécurité optimisée.
- Utiliser des adresses mails « poubelles » c'est à dire qui ne servent qu'à l'installation des applications sans lien direct avec l'identité.
- Utiliser des applications que l'on peut protéger par des codes confidentiels.

Le risque zéro n'existant pas, c'est la multiplication des points de vigilance qui permettra de protéger les données personnelles des élèves et éviter qu'elles ne soient utilisées à des fins non connues.

Quels sont les enjeux d'une formation d'un citoyen numérique avisé ?

Il est plus que jamais essentiel d'éduquer les élèves au respect de ce droit fondamental qu'est le droit à la protection des données. À l'ère numérique, l'éducation à un **usage citoyen, responsable et éthique** des nouvelles technologies constitue une priorité d'action, tout particulièrement auprès des jeunes en âge scolaire.

Un référentiel international de formation à la protection des données à été rédigé afin de permettre aux jeunes d'acquérir une connaissance et une compréhension critiques de droits et responsabilités numériques, développer auprès d'eux une démarche réflexive sur les usages qui sont faits des données personnelles, sensibiliser sur les risques et enseigner les pratiques permettant de se mouvoir dans l'environnement numérique avec confiance, lucidité et dans le respect des droits de chacun : tels sont en effet les **objectifs de formation à atteindre.**

Plus d'informations : http://eduscol.education.fr/cid129745/le-referentiel-cnil-de-formation-des-eleves-a-la-protection-des-donnees-personnelles.html

Quelles sont les limites ?

La principale limite concerne le « bridage » des objets connectés ou des applications sans la transmission d'informations personnelles. Sans créer de compte ou sans transmettre certaines informations, les objets ne permettront pas d'exploiter

toutes les fonctionnalités possibles ou seront même inutilisables. Il s'agira d'user d'intelligence pour transmettre des informations qui en révèle le moins possibles (ou qui ne soient pas « vraies ») sur notre privée et celles de nos élèves.

De plus, de la même manière qu'on ne parle plus d'«objet électrique », l'utilisation de la locution « objet connecté » est déjà presque obsolète. Ainsi, dans un futur proche nous ne parlerons plus de montre connectée mais d'une montre, tout simplement, son caractère connecté étant devenu une évidence.

La capacité d'intelligence est souvent attribuée à ces objets. Or c'est encore loin d'être une généralité. Un objet intelligent se distingue d'un simple objet connecté par sa capacité à interpréter de la data afin d'anticiper et de prédire des comportements. Lorsque les objets connectés seront réellement dotés de la capacité d'apprendre, de s'adapter à l'utilisateur et à son environnement, lorsqu'ils évolueront par expérience et non par paramétrage, l'utilisation du terme « Smart » ne sera alors plus abusive. Dès lors ces appareils pourraient influencer fortement nos comportements voir même les guider. La problématique du libre arbitre dans les choix de notre mode de vie sera fortement questionnée.