



La vie privée des jeunes est-elle protégée sur Internet ?

Pour plus de sécurité, adoptez les réflexes CASES !

Les enfants grandissent au milieu de valeurs en pleine mutation

Les parents et la société occupent une grande part dans la vie d'un enfant. Ils influencent son identité en pleine formation. Mais que signifie « identité » pour la jeune génération Internet ? De nos jours, Internet et les technologies numériques poussent l'identité de chacun sous les feux de la rampe comme jamais auparavant. Les enfants ne connaissent qu'une infime partie des données les concernant stockées numériquement. Si des parties de ces informations parviennent au grand public, elles deviennent des éléments de l'identité numérique de l'enfant, qu'il le veuille ou non.

Comment les enfants et les adolescents peuvent-ils révéler autant d'informations personnelles sur Internet ? Beaucoup d'adultes se posent cette question. Jamais auparavant une quantité aussi considérable de données personnelles n'a été accessible à un nombre si important de personnes. Mais les enfants et les



adolescents sont-ils les seuls responsables de ces révélations de données privées et, par conséquent, de la violation de leur intimité ? On trouve aussi sur le réseau des réseaux des informations sur des personnes qui ne partagent pas le style de vie de la génération Internet. Incriminer l'attitude des jeunes sur le réseau comme cause d'une possible perte de vie privée est un raccourci trop rapide.

Les États-Unis et l'Union européenne illustrent parfaitement comment les droits en matière de protection des données en ligne peuvent être interprétés différemment selon les pays. Si l'Europe donne la priorité à

la protection de la vie privée, les États-Unis préfèrent mettre l'accent sur la liberté d'expression et permettent le stockage massif de données privées par les entreprises. L'humanité est encore loin d'une disposition mondiale sur la manière de protéger les données.

Par ailleurs, personne de la génération Internet n'a le recul suffisant pour analyser les répercussions d'une identité publique sur Internet durant toute une vie et en faire part. Il est toutefois hors de question que les jeunes organisent leur vie de façon déterminante via le monde numérique. Ils doivent donc être prêts d'une façon ou d'une autre à faire face aux

conséquences d'un monde numérique perméable tel qu'il existe actuellement.

Les enfants n'ont pas encore l'esprit critique nécessaire pour déterminer les données pouvant être dévoilées sur le Net et l'apparence qu'aura leur identité des années plus tard. Les jeunes ont une préoccupation : vivre leur vie. Pour eux, il est important de savoir combien d'amis ils ont sur Internet, quels réseaux sont « in » et qui est en ligne en ce moment. Aucun adulte ne peut prévoir actuellement les conséquences que le flux de données aura dans vingt ou trente ans.

La question initiale - comment les enfants peuvent-ils révéler autant d'informations sur eux sur le Net ? - devrait plutôt être formulée comme suit : que faisons-nous, en tant qu'adultes, pour protéger la vie privée des enfants et des adolescents dans le cadre de la société du savoir actuelle ?

Comment les données arrivent-elles sur le Net ?

Quand un jeune arrive dans la vie active aujourd'hui, des centaines d'enregistrements numériques existent déjà à son propos. Ces documents numériques sont entre les mains les plus diverses. Le jeune ignore quelles données existent et qui les possède. Même une recherche de tous les documents numériques existants serait impossible

Les effets à long terme rarement pris en compte

Chaque jour, des adultes prennent des décisions sur la publication de données personnelles d'enfants et d'adolescents. Des personnes et organisations tierces ont alors un grand contrôle sur des données privées. Nous ne sommes qu'au début de la société du savoir numérique. Une personne née à l'époque numérique n'est pas encore arrivée au bout de sa vie d'adulte. Personne ne peut encore parler des répercussions de traces de données numériques sur toute une vie. Mais nous savons et voyons que la mise en réseau de ce monde s'accélère chaque année. Il faut donc s'inquiéter des conséquences possibles à long terme d'un manque de sécurité des données.

La confiance au cœur du problème de la vie privée

Le but des enfants et adolescents sur Internet est d'être en réseau et de communiquer. Ils ne savent pas qu'ils sont aussi automatiquement reliés à un grand nombre d'entreprises, organisations et institutions publiques. Ces derniers disposent d'une quantité de données sans cesse croissante sur les jeunes. Or, il n'y a que peu de lois sur la protection de la vie privée, surtout en ce qui concerne les enfants et les adolescents. À ce propos, les lois européennes de protection des données sont encore assez strictes.

Demande de protection centralisée

Les parents et enseignants constituent la première protection autour de la jeune génération numérique. Ils sont les mieux placés pour expliquer aux enfants et adolescents la valeur de la vie privée et la protection de leur propre identité. Les entreprises informatiques représentent une autre protection importante. Par une interface utilisateur conviviale et des investissements ciblés dans la sécurité des produits, elles peuvent contribuer largement à la protection des données. La législation est une troisième protection. Une série de lois bien pensées peut participer à une meilleure protection de la vie privée des enfants et des adolescents. Mais il faut noter ici qu'Internet ne connaît pas de frontières géographiques ou politiques.

concrètement. Où commencer ? Où s'arrêter ? Quelles sont les pistes correctes ?

Les jeunes Luxembourgeois interrogés sur les informations disponibles sur eux en ligne donnent les réponses suivantes : mon profil Facebook avec des informations sur mes loisirs et mes amis, mon blog sur lequel je décris ce que je fais, mon album photo en ligne. Une recherche du nom par Google répertorie certes des milliers de résultats mais seuls les premiers sont intéressants en général. Ce sont ici les informations traditionnellement répertoriées par les jeunes. Mais il n'est pas rare de trouver aussi quelques résultats où des amis donnent des informations sur le jeune. Et la liste semble ainsi être close. Les jeunes pensent avoir leurs données sous contrôle. Un sentiment de sécurité illusoire !

Les moteurs de recherche tels que Google sont loin de divulguer toutes les informations numériques d'une personne consignées sur Internet. Il existe des services et réseaux en ligne qui bloquent les webcrawlers d'un moteur de recherche qui parcourent Internet pour dénicher des informations. Ces données invisibles pour les moteurs de recherche ne sont accessibles qu'aux personnes qui s'inscrivent auprès d'un tel service selon certaines règles pour des sommes souvent rondellettes. Ces données du « deep web » ne remontent à la surface d'Internet que par moment, par exemple à la

suite de failles dans les systèmes ou d'erreurs d'utilisation humaines.

Les informations arrivent de plus en plus souvent par des terminaux Internet mobiles comme les téléphones portables. Il suffit d'un clic pour retrouver sa photo sur Internet. Mais ce n'est pas tout. Ces photos sont souvent pourvues d'une identification par l'utilisateur, comme par exemple le nom de la personne photographiée ou un commentaire. Dans le jargon, on parle de tagging. Ces légendes facilitent certes la recherche de données par des amis mais ne vont certainement pas dans le sens de la protection des données.

Le moteur de recherche visuel Riya permet de relier des photos en ligne non balisées avec des photos déjà identifiées. Des données apparemment sans aucun lien peuvent ainsi être assemblées facilement et rapidement. Le regroupement d'informations ainsi obtenu en dévoile bien plus que ne le ferait une information isolée.

Même la génération plus âgée contribue inconsciemment à amplifier le problème de la protection des données. Les parents inquiets veulent protéger leurs enfants par des filtres, caméras de surveillance, détecteurs de mouvement, webcams ou puces RFID

intégrées dans le téléphone mobile pour savoir où leurs enfants se trouvent. Les données restantes peuvent alors facilement devenir partie intégrante des dossiers numériques d'un enfant. Avant de prendre les mesures susmentionnées, les parents hésitent souvent entre une sécurité accrue et la perte de vie privée, mais les conséquences numériques possibles à long terme interviennent rarement dans la réflexion.

Qu'en est-il des données des patients ? Dans certaines circonstances, les établissements médicaux sont autorisés à partager des données d'un dossier médical avec des tiers. C'est utile tant que cela sert à accélérer le processus de guérison d'un enfant, par exemple. Mais ces enfants devenus adultes n'ont aucun contrôle de ces données et encore moins connaissance de leur existence ou ignorent qui possède ces informations.

Les enfants peuvent-ils réellement s'y retrouver ?

Les jeunes ont du mal à comprendre les intérêts économiques. Ceci est d'ailleurs également valable pour bon nombre d'adultes. Les prestataires en ligne sont nombreux à tenter de convaincre enfants et adolescents à coup d'astuces et de manipulations psychologiques de révéler des données privées. La

jeune génération ne saisit que rarement les intérêts économiques complexes qui se cachent derrière l'accumulation d'informations par un réseau social comme Facebook. Les enfants sont-ils dans ce cas réellement responsables de la divulgation d'informations ?

De plus, enfants et adolescents font la plus grande confiance aux services sur Internet. Interrogez simplement votre fille de dix ans à ce sujet. Connaît-elle les « conditions générales » du site de jeux en ligne sur lequel elle se trouve ? Les enfants ne savent pas ce que cela signifie. Ils sont encore moins nombreux à lire les petits caractères du site.

Même si les conditions générales d'un service

reconnaissent la protection des données de l'utilisateur, pratiquement personne ne sait qu'une entreprise peut modifier ses conditions générales à tout moment. La pression économique suffit souvent ici.

Le cas ChoicePoint

En 2005, l'entreprise américaine ChoicePoint devait avertir 100 000 clients que des données privées avaient été transmises par inadvertance à des escrocs. Le point désagréable dans cette histoire pour ChoicePoint ? L'entreprise était absolument inconnue des destinataires du courrier. Aucune de ces personnes n'avait autorisé l'entreprise à créer un dossier numérique à son sujet et encore moins à

vendre ces informations à des tiers.

ChoicePoint, entreprise cotée en Bourse sise dans l'État fédéral américain de Géorgie, gagne de l'argent en rassemblant des informations sur des personnes. Et l'entreprise avait vendu des données involontairement à des escrocs. 800 personnes ont été victimes d'un vol d'identité à cause de cette erreur. Malgré une amende de plusieurs millions, l'entreprise a racheté plus de 50 entreprises comparables trois ans plus tard, en 2008. Difficile d'imaginer ce qu'il se passera lorsque des entreprises comme ChoicePoint commenceront à utiliser les données collectées sur une personne.

Retrouvez les dossiers, fiches thématiques alertes et actualités sur:

www.cases.lu