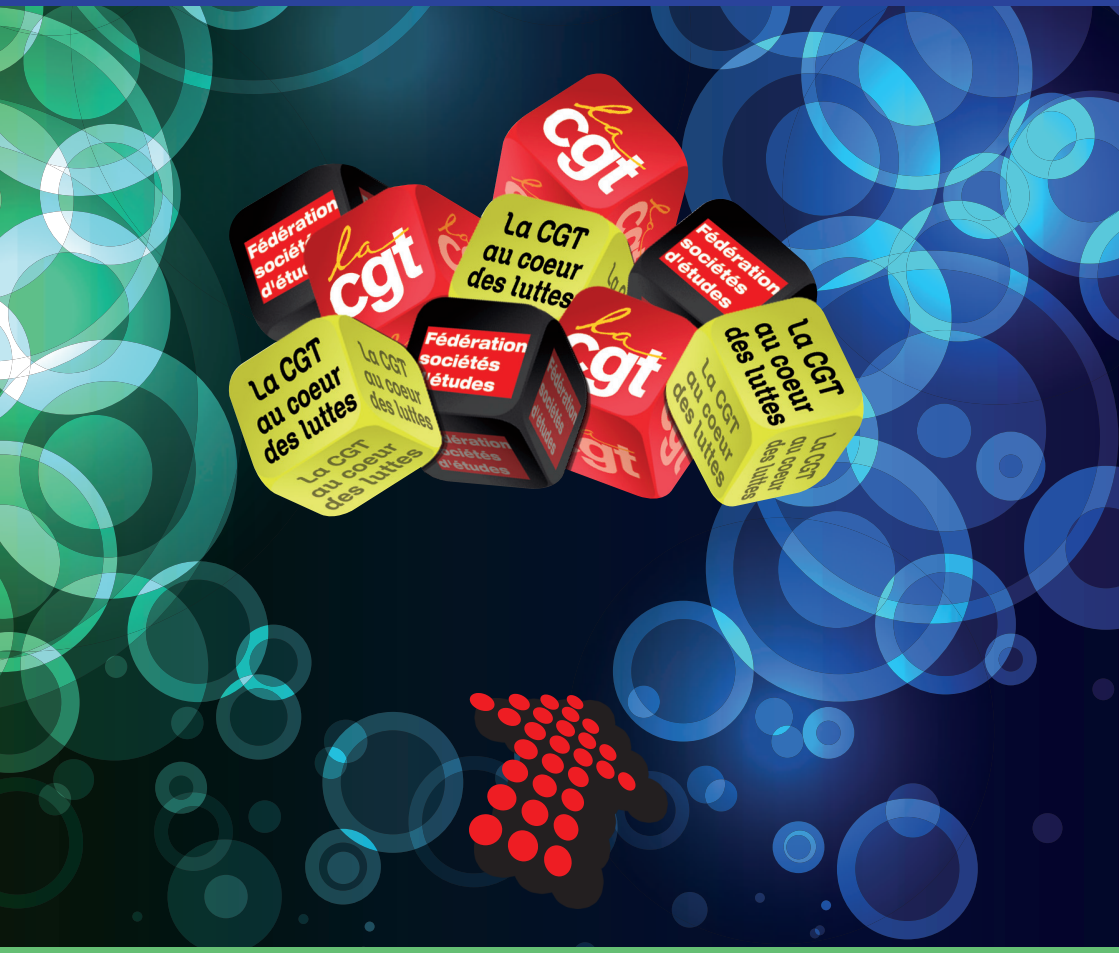
FACE A LA SOCIETE DU NUMERIQUE, NOS DONNEES PERSONNELLES SONT-ELLES SUFFISAMMENT PROTEGEES ?

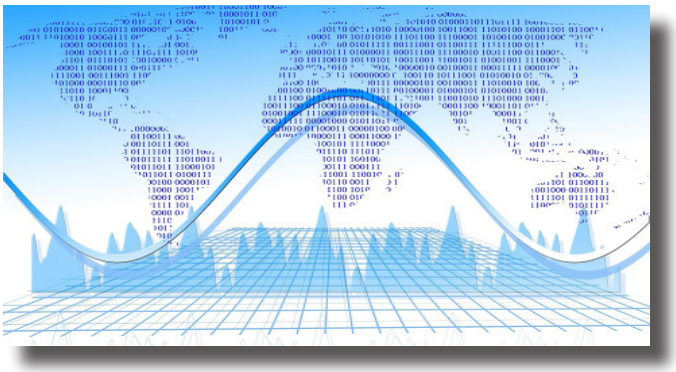


la cgt Fédération sociétés d'études

Fédération CGT des Sociétés d'Etudes

263, rue de Paris - Case 421 - 93514 Montreuil - Cedex
Téléphone : 01 55 82 89 41 Fax : 01 55 82 89 42
E-mail : fsetud@cgt.fr - Site Internet : www.soc-etudes.cgt.fr

Sommaire



Avant-Propos

C'est l'intitulé d'un colloque organisé le 28 Juin 2017 par Indecosa-CGT, l'association de consommateurs de la CGT. Cette rencontre a le mérite de lier la question des usages du numérique (ici de la gestion des données) avec celle de la défense des consommateurs salariés. En croisant l'analyse usagers-travailleurs du numérique et consommateurs-producteurs, nous abordons ici, d'abord et avant tout, la question des libertés individuelles et collectives sur ce nouvel espace qu'est internet. Nous avons donc décidé, face aux enjeux fondamentaux de cette nouvelle problématique, de retranscrire les interventions qui ont eu lieu lors de cette rencontre.

« Aujourd'hui, le numérique est partout et modifie peu à peu nos actes de la vie quotidienne. Très souvent, cela se traduit par la disparition de certaines démarches, par exemple, la déclaration d'impôt par internet au détriment du support papier. L'avènement de cette nouvelle société suscite de nombreuses inquiétudes notamment sur le sort réservé aux données conservées par les outils numériques. Ces craintes se sont révélées exactes puisque l'on a pu voir avec l'affaire Snowden, comment les Etats-Unis ont pu espionner impunément le monde entier. Pour rassurer les « e-consommateurs », la France s'est donc dotée en 2016 d'une législation pour mieux encadrer notre société numérique. Services publics, recherche, e-sport ... les secteurs abordés sont nombreux et la loi réforme plusieurs codes (tourisme, consommation, postes et télécommunications ou encore relations entre le public et l'administration). Plusieurs dispositions touchent à la protection des données personnelles (mort numérique, droit à l'oubli des mineurs, portabilité des données); Elles ne font qu'anticiper la législation européenne, adoptée en avril 2016, qui entrera en vigueur en mai 2018. Pourtant, lorsque l'on regarde de plus près cette règlementation « renforcée », on se garde bien d'aller trop loin pour ne pas heurter les « tenants » de cette nouvelle économie très lucrative.

*Dans certains secteurs comme le « e-santé », on est conscient des risques mais on ne peut pas trop « bunkeriser » pour ne pas effrayer nos chères Startup. Pourtant, les risques de piratage et de vol de nos données personnelles médicales sont réels et les cybercriminels sont bien conscients de leur valeur. Un vol d'un numéro de sécurité sociale a des conséquences bien plus graves qu'un vol de numéro de carte bancaire, permettant par exemple l'usurpation d'identité***. »**

Introduction de Arnaud FAUCON

Secrétaire National INDECOSA-CGT

Bonjour à tous,

Merci de votre venue. Nous allons aborder aujourd'hui le problème de l'exploitation de données personnelles avec la montée en puissance du « tout connecté ».

Cela concerne en particulier les objets qui nous entourent dans notre vie quotidienne et dont les données sont collectées par des entreprises via internet. Trop souvent, cette « captation » d'informations se fait à l'insu des individus sans leur consentement préalable. Dans une affaire récente, un concepteur de logiciels a mis en évidence, via son blog, que des téléviseurs LG espionnaient les téléspectateurs. L'entreprise LG s'est finalement excusée après s'être attiré les foudres des internautes. Elle s'est engagée par la suite à remédier à cette « anomalie ».

A l'opposé de l'entreprise Coréenne, un géant du net continue d'exploiter la vie privée des personnes malgré les rappels à l'ordre. Depuis des années, INDECOSA-CGT dénonce les pratiques de Google avec son dispositif « street view ». Le principe est de faire circuler des voitures censées prendre des images utilisées par son service de cartographie. En réalité, ces véhicules ne se sont pas contentés de capter des photographies. Des données Wifi relatives au contenu des communications, c'est-à-dire les échanges entre les ordinateurs et les points Wifi ouverts, ont également été enregistrés. Or, cette collecte n'était pas mentionnée dans la déclaration de Google à la CNIL.

Malgré la mise en demeure de la CNIL, Google n'a pas daigné répondre et s'est vue condamnée à payer une amende très faible de 100 000 euro au regard de la puissance économique du groupe. Néanmoins, Google ne désarme pas puisqu'il a fait un recours au Conseil d'Etat pour faire annuler cette sanction. De plus, le géant américain traîne aussi les pieds sur le « droit à l'oubli ». Ainsi, encore aujourd'hui, des internautes qui tentent de faire valoir ce principe auprès du moteur de recherche se retrouvent à nouveau « publiés » après plusieurs mois de silence.

D'ici 2020, plus de 80 milliards de produits seront ainsi connectés à internet. Cela va concerner les ordinateurs, les smartphones, les tablettes, les

montres connectées… Face à cette situation, le consommateur est inquiet mais pas naïf. Une étude commandée par INTEL montre que 81 % des français craignent que les données collectées par leurs objets connectés soient utilisées à des fins marketing et 90 % se préoccupent du piratage. Dans le même temps, ils sont plus de 6 sur 10 à être prêts à vendre ou échanger lesdites données...

Face à cette situation, les pouvoirs publics ont souhaité un renforcement de la législation. Ainsi, la loi informatique et libertés complétée récemment par le règlement européen (application en 2018) forment désormais un cadre juridique qui appréhende une bonne partie des problèmes liés aux données personnelles : Parmi les principales garanties apportées par ce régime juridique, figure la loyauté de la collecte de données par les objets connectés : elle doit être proportionnée et pertinente par rapport à l'usage prévu.

En d'autres termes, les concepteurs d'applications qui récoltent des données personnelles et les traitent, ne peuvent plus avoir un raisonnement du type « j'ouvre mon service, je collecte de multiples informations sur les utilisateurs et l'on verra bien ensuite tout ce que l'on pourra en faire avec ».

C'est d'autant plus vrai que le caractère proportionné et pertinent des données collectées par rapport à l'usage prévu (la finalité du traitement de données personnelles) est renforcé par le règlement européen sur la protection des données qui introduit deux notions fondamentales à prendre en compte: celles du «privacy by design» et du «privacy by default».

Les traitements de données personnelles doivent normalement faire l'objet de formalités déclaratives ou, pour certains traitements plus sensibles, de demande d'autorisation auprès de l'autorité de contrôle (comme la CNIL en France).

Le règlement européen s'appuie lui sur une logique de responsabilisation des entreprises qui seront dispensées désormais de ces déclarations aux autorités de contrôles quand le règlement sera d'application effective en 2018. Pour accompagner cette dispense de déclarations, les missions et les pouvoirs des autorités de contrôle seront renforcés.

Aujourd'hui, les autorités de contrôle peuvent déjà mener des audits réguliers et elles le font régulièrement chaque année. La CNIL (Commission Nationale Informatique et Libertés) est d'ailleurs particulièrement attentive aux traitements mis en oeuvre par les objets connectés puisque dans le

cadre de l'Internet Sweep day, elle a prévu de lancer un vaste contrôle sur différents sites et objets connectés.

L'organisme va notamment pouvoir vérifier trois éléments essentiels :

- Premièrement, l'information délivrée aux utilisateurs est-elle suffisamment claire et précise ?
- Deuxièmement, le niveau de sécurité des flux de données est-il satisfaisant?

Enfin, quel degré de contrôle l'utilisateur garde-t-il sur ses données ? Il doit donner explicitement son consentement, pouvoir paramétrer l'accès à ses données et ces dernières doivent être «purgées» au bout d'une durée.

Comme nous l'avons vu précédemment, les sanctions n'étaient jusqu'à aujourd'hui guère dissuasives. Sur ce point, le règlement européen apporte un vrai changement: les amendes pourront atteindre 20 millions d'euros ou 4 % du chiffre d'affaires mondial de l'entreprise fautive, étant précisé que l'autorité de contrôle pourra retenir la somme la plus élevée des deux. De plus, ce n'est plus uniquement le concepteur de l'application, du service, ou de l'objet connecté qui peut être mis en cause : ses sous-traitants sont aussi ciblés.

A plus long terme, l'un des principaux dangers que j'identifie concerne l'utilisation d'objets connectés et d'applications ayant trait à la santé et l'usage que pourraient faire les compagnies d'assurance des données ainsi récoltées.

Aujourd'hui, les applications ont un caractère ludique et appréciées des consommateurs. Si à l'avenir l'usage de ces dispositifs se généralise, les personnes qui en refusent l'usage pour justifier de leur bonne santé ou de leur hygiène de vie ne risquent-elles pas d'être tout bonnement exclues par leur assurance ou se voir appliquer des surprimes ?

Enfin, comment s'y retrouver face à une multitude d'offres ? Probablement le développement de normes, sur le modèle de celles mises en place par l'ISO, qui permettraient d'identifier les services qui sont exemplaires du point de vue de la protection des données personnelles et du respect de la législation en vigueur. La conformité à ces normes donnerait confiance au consommateur, de plus en plus préoccupé par ces questions.

La problématique des données du point de vue syndical. Quels changements pour les entreprises du numérique et les salariés ?

Jean-Baptiste Boissy, Conseiller fédéral pour la Fédération CGT des Sociétés d'Etudes

La CGT commence à s'ouvrir depuis quelques années à la question de la numérisation et de son impact sur l'économie et les salariés. Nous saluons donc l'initiative d'Indecosa qui s'inscrit dans ce cadre. Rappelons qu'il ne s'agit pas d'une seule et unique problématique du numérique mais de thèmes variés qui touchent l'ensemble de l'économie et de la société.

Parmi ces problématiques multiples, on peut citer au niveau économique :

- la question de l'automatisation et des prévisions de destructions et/ou de transformations des emplois ;
- l'influence des outils et usages numériques sur les conditions et l'organisation du travail ;
- les stratégies de communication ;
- l'usage de l'information, notamment avec les réseaux sociaux ;
- l'apparition d'une nouvelle économie de plateformes qui remet en cause le statut du salariat ;
- la constitution d'une filière particulière du numérique qui couvre l'ensemble de la chaîne de production, de la fabrication manufacturière des équipements et la gestion des infrastructures jusqu'à la vente des produits électroniques et l'ingénierie (conception de logiciel, etc.).

Il ne faut pas perdre de vue ici que les questions liées au travail sont aussi étroitement liées à l'impact social du progrès technique et c'est sur ces enjeux sociétaux du numérique que la question de la protection des données personnelles prend tout son sens. C'est pourquoi notre analyse doit s'effectuer sur plusieurs fronts qui vont au-delà du seul périmètre de l'entreprise et qui demandent une réflexion transversale : transversale entre les organismes de la CGT, entre les différents acteurs sociaux et enfin, par rapport à l'habituelle opposition entre travailleur-producteur et consommateur-usager.

Il s'agit donc de problématiser cette question de la gestion des données à partir de notre point de vue syndical en tant que travailleurs qui défendent

leur intérêt de classe, mais aussi en tant qu'individus usagers et citoyens attachés aux libertés individuelles.

On peut d'abord souligner que la protection des données personnelles n'est pas seulement une problématique interne au numérique, mais s'insère aussi dans un contexte politique particulier que ce soit au niveau national dans une période de recul des libertés (on l'a vue avec l'état d'urgence, la répression anti-syndicale et toutes les atteintes à la liberté de manifester pendant la Loi Travail) et au niveau international où l'actualité des dernières années a été marqué par la chasse internationale aux lanceurs d'alerte. J'entends par là que notre engagement à défendre la liberté syndicale et l'ensemble des libertés (d'opinion, d'expression, au respect de la vie privée etc…) passe aussi par cette question de la protection des données personnelles et collectives, car nous verrons que cette question se pose aussi dans le cadre des données internes aux sections syndicales en entreprise.

Autre constat important : la collecte d'informations, qui jadis relevait du monopole d'état (qui en principe devait rendre des comptes aux citoyens), est aujourd'hui entre les mains de grandes entreprises (comme Google, Facebook, Twitter) qui, elles, agissent au nom d'intérêts privés. Ce constat nous pousse à nous interroger sur les limites que l'on doit fixer face aux entreprises et d'un point de vue théorique sur la question de l'éthique des TIC (Technologies de l'information et de la communication) et sur l'usage du progrès technique.

1) La collecte de données personnelles comme stratégies commerciales suivant des intérêts privés

Un rapport du CESE de 2015 notait que « depuis les origines de l'humanité et jusqu'en 2003, l'humanité avait produit 5 exaoctets de données numériques, soit 5 milliards de milliards d'octets. En 2010, il suffisait de 2 jours pour produire le même volume et depuis six ans, le poids de la data dans les communications électroniques augmente de 5 points par an ». Aujourd'hui, une requête sur internet peut générer une analyse de données sur 200 millions de sites web, 90% de la data disponible dans le monde a été créé depuis 2 ans.

Ce qu'il faut bien comprendre ici avec ces chiffres, c'est que nous ne sommes pas seulement face à une révolution numérique dans le sens de l'apparition de nouveaux outils et de nouvelles pratiques de production mais face à une révolution informationnelle où on a créé une nouvelle ressource qui est la donnée, quelle qu'elle soit.

Cette donnée est manipulable à des fins commerciales, d'abord publicitaire et marketing, puisque nos visites sur un certain nombre de pages renseignent les grands groupes sur nos goûts et nos centres d'intérêt et leur permettent ensuite de nous cibler avec des publicités.

La collecte et le traitement de données fait émerger de nouveaux secteurs d'activité de datafication qui visent à transformer la donnée comme matériel brut de base en data ou en informations. C'est-à-dire une information numérique, codée par la machine, mémorisée par le système informatique et transmissible ensuite sur le web, stockée dans des centres spécifiques (data centers). Le Big Data représente l'ensemble des technologies, infrastructures et services qui gèrent le cycle de transformation de la donnée en information et sa diffusion.

Autre aspect problématique : la revente d'informations. Avant d'être un réseau social, Facebook est avant tout une entreprise. Elle peut vendre les informations collectées sur nous à n'importe qui, comme l'a montré le scandale de l'espionnage mondial de la NSA. L'entreprise avait même prévu en 2009 de garder une licence sur tout le contenu produit, c'est-à-dire d'avoir des droits sur les photos et les textes que nous postons par exemple. Il en va de même pour les données produites par les salariés qui peuvent être soumises au piratage par l'intermédiaire de logiciels espions, où le piratage économique est lui-même intégré depuis longtemps comme stratégie commerciale à l'image des cyberattaques qui ont impacté une quarantaine de cabinets spécialisés en fusions-acquisitions en 2016.

On peut donc parler d'un marché de la donnée à très forte valeur ajoutée. Le chiffre d'affaire du Big Data représentait 6.3 milliard de dollars en 2012 et 25 milliards en 2016. Le Syntec Numérique, syndicat patronal de l'ingénierie informatique, ne s'y trompe pas quand, dans une note de janvier 2017, il se sert des données comme d'un argument supplémentaire à la déréglementation des marchés : « Après avoir établi la liberté de circulation pour les personnes, les biens, les services et les capitaux, l'heure est venue d'établir la 5ème liberté de circulation, celle applicable aux données, qui sont la matière première du XXIème siècle ».

A travers l'exploitation des données, on assiste également à un autre processus : l'usager n'est plus seulement un consommateur mais aussi un producteur. L'émergence du marché de la data bouleverse en effet la frontière entre producteur et usager. Ce phénomène porte un nom, c'est le

digital labor. On pourrait traduire ce concept par travail numérique mais on est face à un travail qui n'a pas de reconnaissance juridique et qui n'est pas produit au sein des lieux de production. Il s'agit, pour faire vite, du travail des usagers du net, à savoir les activités numériques quotidiennes des usagers sur les plateformes sociales, les objets connectés et les applications mobiles. Les posts, les photos, les saisies, les connexions, tout cela produit de la valeur qui est ensuite captée par les grandes entreprises, en premier lieu les GAFA. Il s'agit juste d'une récupération marchande des flux internet à contre-courant de l'idée de partage, des communs.

2) La collecte des données s'effectue aussi comme stratégie de contrôle sur les salariés à travers la cybersurveillance et des stratégies managériales

On parle souvent des données personnelles avec l'image de l'usager internet qui postent des informations sur sa vie privée sur les réseaux sociaux ou qui remplit des formulaires en donnant son adresse, son nom, son prénom ou des renseignements personnels. Mais cette question est aussi au cœur de l'entreprise où, là, le traitement des données aboutit à un contrôle accru des salariés.

Ce contrôle ne s'effectue pas seulement par la surveillance mais aussi par des dispositifs d'individualisation et d'aliénation des salariés par de nouvelles pratiques managériales et tout un travail idéologique de redéfinition du travail. Soulignons d'abord que la gestion de données est une nouvelle tâche en tant que telle et pas seulement pour les salariés du numérique. Les courriels, par exemples, sont aussi des données et on sait à quel point, dans l'économie de service, leur gestion est devenue importante. On aboutit à un phénomène de hyper-connexion d'autant plus important qu'aujourd'hui le salarié n'est plus posté mais possède son outil de production avec lui grâce aux objets connectés qui le suivent partout, y compris en dehors du lieu et des heures de travail. On peut donc considérer que la donnée dévore le travail du salarié comme le logiciel dévore le monde selon l'expression consacrée.

C'est autour de cet enjeu de la déconnexion que se concentre aujourd'hui notre intervention syndicale, contre ce qui apparait comme du travail dissimulé, non rémunéré et non pris en compte et qui remet en cause la notion même de temps de travail tout en imposant des charges supplémentaires qui produisent plus d'exploitation et plus de souffrances au travail. L'augmentation des charges de travail couplée à l'usage des objets connectés comme outil de production de données possède son

pendant idéologique avec le discours sur l'autonomie qui permet de justifier la destruction des cadres collectifs de travail, de l'espace et du temps de travail et qui impose, en dernier lieu, un contrôle « soft » sur le salarié en le rendant faussement responsable d'un travail qui brouille le lien de subordination économique.

En parallèle, on assiste à la multiplication des techniques et des outils de surveillance. Je ne reviendrais pas en détail sur l'ensemble de ces dispositifs mais on peut lister rapidement :

- les dispositifs biométriques qui collectent vos empreintes digitales notamment ;
- l'espionnage de la messagerie électronique et des connexions Internet ;
- le contrôle de l'accès aux fichiers informatiques ;
- l'écoute des messages vocaux et SMS laissés par un salarié sur le téléphone professionnel d'un collègue et des communications téléphoniques ou des numéros composés grâce à l'accès des autocommutateurs ;
- la vidéosurveillance ;
- et la géolocalisation.

On a donc bien un double contrôle : par la persuasion d'un côté et par la contrainte de l'autre. Qu'en est-il de la réglementation ?

Pour l'hyper-connexion due à l'usage des objets connectés, le nouveau droit à la déconnexion est un premier pas vers un meilleur encadrement mais reste difficilement applicable dans la pratique et ne pose pas le problème fondamental des charges de travail.

Sur les dispositifs de contrôle, la loi « informatique et libertés » du 6 août 2004 permet de sanctionner les manquements à hauteur de 3 ans d'emprisonnement et de 300.000€ d'amende. Normalement les salariés doivent être informés des dispositifs mis en place et des modalités de contrôle de l'utilisation d'internet. Cette information passe par la consultation et l'information du Comité d'Entreprise, par l'information des salariés sur la finalité du dispositif de contrôle et sur la durée pendant laquelle les données de connexion sont conservées. Toute absence de déclaration rend le dispositif de surveillance illégal. La Cnil fait figure de gardienne du temple, une sorte d'inspection du travail numérique, qui permet de réguler ces techniques sans que l'on sache réellement quelles sont les mesures de contrôle concret ni l'ampleur des contournements vis-à-vis de la loi par les entreprises.

3) On observe une asymétrie au niveau de la protection des données entre entreprises et salariés

Toutefois la législation laisse encore beaucoup de pouvoir à l'employeur. L'employeur peut surveiller la consultation des sites internet d'un salarié en inspectant le disque dur de son ordinateur à son insu. Même chose pour la consultation de la liste des favoris sur les navigateurs internet ou également sur une clé USB qui, dès lors qu'elle est connectée à un outil informatique mis à disposition par l'entreprise pour l'exécution du contrat de travail, peut être inspecté en son absence. Il en va de même enfin pour les courriels adressés par le salarié à l'aide de l'ordinateur professionnel, ce qui pose souvent problème en ce qui concerne la communication syndicale.

La législation donne par contre moins de marge de manœuvre aux salariés quand il s'agit de dénoncer des situations irrégulières et de diffuser des données au nom d'un point de vue éthique ou de l'intérêt général. Je parle ici des lanceurs d'alerte qui sont aujourd'hui largement pénalisés. On l'a vu avec le cas scandaleux de l'affaire Tefal où a été condamnée une inspectrice du travail, Laura Pfeiffer, pour violation du secret professionnel et recel de documents volés.

Elle avait divulgué des mails, par l'intermédiaire d'un salarié, qui démontraient l'existence de pressions de la multinationale sur sa hiérarchie pour l'écarter de son poste alors qu'elle gênait l'entreprise en souhaitant faire respecter un accord sur les 35 h. Récemment a été mis en cause la directive européenne sur le secret des affaires qui, sous prétexte de limiter la concurrence déloyale ou l'espionnage économique et industriels et de garantir la propriété intellectuelle des brevets et autres marques, limite surtout la possibilité de révéler des données sensibles soumises au secret économique.

4) Peut-on limiter l'exploitation des données personnelles en amont dans le process de production ?

A notre niveau syndical et sur le périmètre de l'entreprise, la gestion des données, on l'a vu, est un enjeu socio-économique majeur. L'explosion des données de ces dernières années implique une réorganisation de la production et de l'organisation du travail. A la question de la régulation juridique répond aussi celle de la réglementation économique. Il est possible d'agir sur la gestion des données en amont, directement dans le processus de production.

Des efforts de régulations commencent à naitre. Le Parlement européen

a adopté un règlement général sur la protection des données ou GDPR (General Data Protection Regulation) début 2016 pour renforcer la protection des données personnelles face à la numérisation de l'économie. Sa mise en application n'interviendra qu'en 2018. L'idée est d'aboutir à une harmonisation des normes européennes en la matière en influant directement dans le monde de l'entreprise notamment à travers :

- La régulation des relations entre entreprises et utilisateurs : toute entreprise située hors de l'UE doit respecter le GDPR dans la gestion des données appartenant aux résidents de l'UE. Les utilisateurs doivent consentir à l'utilisation ou au stockage des données privées par une entreprise, de même qu'il a un droit à la suppression de ses données personnelles. L'entreprise doit également permettre la portabilité des données personnelles.
- Les entreprises sont dans l'obligation de mettre en place des mesures techniques et organisationnelles pour garantir, par défaut, un traitement des données limité strictement aux seules données nécessaires au regard de leurs besoins (c'est la notion de « Privacy by Design»).

Ce règlement concerne la relation entre entreprises et consommateurs mais évacue la question de la gestion des données dans l'entreprise et des rapports de force à ce niveau entre direction et salariés. Au niveau salarial, aucune disposition ne prévoit de dialogue social. Les délégués à la protection des données (Data Privacy Officer) qui seront les référents pour assurer la bonne mise en œuvre et le contrôle des traitements par mandat des utilisateurs et de l'administration seront extérieurs à l'entreprise. La différence de législations du travail entre pays européens empêche une harmonisation des règles concernant l'implication des représentants des salariés dans ce processus mais appelle surtout à développer en plus du règlement européen une réglementation nationale prenant en compte le rôle du Comité d'Entreprise ou du CHSCT dans la gestion des données à l'intérieur des entreprises.

Autre problème : personne ne sait réellement comment appliquer cette législation et aucune mesure, ni aucun outil n'ont été mis en place pour favoriser son application. On peut se poser la question de la faisabilité d'une telle mesure qui implique aussi un redéploiement de la formation salariale et une phase d'adaptation qui aujourd'hui est inexistante. Quant à l'impact sur les organisations du travail et sur la production, il est pour le moment inconnu.

Toujours est-il que ce règlement permet de recentrer le débat de la protection des données sur l'entreprise. Pour le moment la législation court

derrière l'innovation permanente des TIC, mais c'est surtout au niveau de la conception, en amont, qu'il faudrait réguler ces TIC. Plusieurs pistes existent : renforcer la responsabilité des entreprises, c'est un premier pas avec la GDPR puisque les responsables de traitement à travers le développement des programmes deviennent les garants de la protection des données traitées et doivent en rendre compte en cas de contrôle. Un certain nombre d'outils de conformité sont d'ores et déjà prévus: processus d'habilitation, certifications, labels, audit de conformité, codes de conduite d'associations ou organismes professionnels soumis aux autorités de contrôle, politiques internes, etc.

On pourrait aussi imaginer que cette question soit traitée dans la RSE (Responsabilité sociale de l'entreprise) à condition que cette dernière ait un caractère contraignant, ce qui n'est pas non plus le cas aujourd'hui.

Enfin il faut développer la notion de Privacy by design, en français la protection intégré de la vie privée (PIVP) ou le respect de la vie privée dès la conception. L'idée est que le cadre légal n'est pas suffisant pour assurer la protection des données privées et doit donc être intégré pour plus de garantie directement dans la conception et le fonctionnement des systèmes, réseaux informatiques, des programmes et des logiciels de traitement des données ainsi que dans l'élaboration de pratiques responsables. L'exigence de protection des données est intégrée directement au produit et devient une exigence centrale d'élaboration. Ce qui passe par le respect de plusieurs principes fondamentaux :

- prendre des mesures proactives et non réactives; des mesures préventives et non correctives;
- assurer la protection implicite de la vie privée;
- intégrer la protection de la vie privée dans la conception des systèmes et des pratiques;
- assurer une fonctionnalité intégrale selon un paradigme à somme positive et non à somme nulle;
- assurer la sécurité de bout en bout, pendant toute la période de conservation des renseignements;
- assurer la visibilité et la transparence;
- respecter la vie privée des utilisateurs.

Il ne faut pas confondre cette notion avec celle de « *Privacy by default* » qui elle est un simple aménagement du produit qui se fait au niveau de la configuration pour éviter notamment les difficultés rencontrées par les utilisateurs pour définir les paramètres de protection de leurs données

personnelles et éviter un usage différent des données. C'est une notion assez floue qui n'indique pas si le paramétrage est automatiquement mis sur un mode protectif ou s'il doit être facilement accessible et compréhensible.

Pour conclure sur ce vaste thème, j'aimerais rappeler à quel point la gestion des données est centrale pour les buts et les moyens du syndicalisme car on touche là au sujet bien plus vaste de l'information et de la communication. Une organisation qui est en mesure de produire des données et surtout de les diffuser largement est capable de décupler la portée de ses actions. Les données ne sont donc pas seulement un marché économique, ni un nouveau facteur de production, il s'agit surtout d'un enjeu stratégique organisationnel que l'on doit s'approprier.

Se déployer sur les réseaux sociaux, développer des applications pour les objets connectés impliquent pour nous de renouveler les supports d'information et surtout d'ouvrir de nouveaux fronts sur des espaces où on est peu présent comme Internet.

Principes de la « Nouvelle approche » au niveau européen

Rémi REUSS

La Commission européenne a mis en œuvre en 1985 une « nouvelle » méthode d'élaboration des directives européennes. Ainsi, les directives fixent de manière réglementaire et obligatoire les exigences essentielles de sécurité, de santé, d'environnement et de protection du consommateur à respecter pour permettre la libre circulation des produits concernés par les directives, dans l'espace européen.

Ces directives se réfèrent aux normes européennes harmonisées pour les spécifications techniques correspondant aux exigences essentielles. L'application de ces normes reste à la discrétion du fabricant, qui peut choisir d'appliquer d'autres spécifications techniques pour satisfaire aux exigences essentielles des directives. L'application des normes européennes harmonisées donne présomption de conformité aux exigences essentielles correspondantes.

Le marquage CE matérialise cette présomption de conformité. Il est apposé sur le produit par le responsable de sa mise sur le marché.

La normalisation volontaire peut proposer des modalités dont la mise en œuvre est à la discrétion des acteurs.

Une norme volontaire est « *un document, établi par consensus par les parties*

prenantes et approuvé par un organisme reconnu, qui fournit, pour des usages communs et répétés, des règles, des lignes directrices ou des caractéristiques, pour des activités ou leurs résultats, garantissant un niveau d'ordre optimal dans un contexte donné ».

Dans ce cadre, la voie de la normalisation volontaire parait bien adaptée en particulier à certains sujets qui peuvent concerner tant le flux que le stock règlementaire. C'est par exemple a priori le cas pour la problématique des objets connectés en général et des objets connectés en santé en particulier.

Depuis la Loi Informatique et libertés de 1978, la nécessité d'encadrer le secteur du numérique, notamment en ce qui concerne la protection des données personnelles s'est accrue. Or, ni la loi pour une République numérique entrée en vigueur en octobre 2016, ni la réglementation européenne qui sera appliquée à partir de mai 2018 (Règlement Général des Données personnelles RGDP) ne semblent satisfaire toutes les interrogations et besoins des consommateurs ; en témoigne notamment l'avis du Conseil National de la Consommation (CNC).

En effet, d'une part, on peut relever l'insuffisance, voire l'absence, d'informations sur la fonctionnalité et la performance de certains objets connectés alors que leur utilisation implique de traiter des données personnelles. Ce constat se manifeste aussi dans le cas des objets connectés en santé (qu'ils soient considérés comme Dispositif Médical ou non) tous ne sont pas réglementés comme les dispositifs médicaux).

D'autre part, le traitement des données personnelles en lui-même pose question : quelles garanties pour les consommateurs ? Les interrogations et inquiétudes portent aussi bien sur le stockage que la finalité de l'utilisation des données.

La réglementation européenne, qui viendra s'ajouter à la Loi pour une République numérique porte sur ces points mais ne règle pas définitivement la question ; en effet des modalités d'application restent à fixer et les obligations mises à la charge des responsables du traitement ne viendront pas nécessairement orienter, éclairer le choix des consommateurs, auxquels incombe donc un lourd travail d'information.

La normalisation volontaire semble ainsi un moyen susceptible d'apporter des réponses à ces deux possibilités. La portée doit cependant être précisée (France, Europe, voir International)

A noter qu'un certain nombre d'initiatives de travaux de normalisation existent d'ores et déjà (privacy by design, cybersecurity, …) ; un travail préalable de cartographie et d'analyse des écarts entre les travaux en cours et les besoins des consommateurs est vraisemblablement nécessaire.

Plus d'informations sur la nouvelle approche :
http://www.francenormalisation.fr/les-acteurs-de-la-normalisation/la-nouvelle-approche/

Plus d'informations sur le comité consommation d'AFNOR
http://www.francenormalisation.fr/gouvernance/comites-consultatifs/

Entretien avec Patricia Faucher, responsable du service juridique de l'Institut national de la consommation (INC), établissement public, industriel et commercial dont les missions sont d'informer les consommateurs et d'appuyer techniquement les associations de consommateurs.

Pourquoi qualifier les données personnelles de « pétrole du 21e siècle » ?

C'est une expression utilisée par la Présidente de la CNIL (commission nationale informatique et libertés). Le développement du numérique, celui des objets connectés, des réseaux sociaux ont permis de collecter énormément d'informations communiqués par les consommateurs et citoyens, ce qui va permettre de cibler les choix, les goûts des personnes dans un tas de domaines comme l'alimentation, la mode, etc. Or, ces données personnelles ont une valeur puisqu'elles vont permettre aux professionnels d'offrir de nouveaux vecteurs, de nouveaux produits, de nouveaux services adaptés aux personnes. On parle donc de pétrole parce qu'elles sont monétisables et qu'elles constituent un grand gisement financier.

D'un côté, les consommateurs veulent être protégés, de l'autre, ils sont très bavards… Jusqu'où l'INC peut-il les protéger ?

Il est de notre responsabilité en tant qu'association de consommateur de sensibiliser les consommateurs à la nécessité d'être vigilants lors de la collecte des données personnelles par exemple. Qui va collecter ces données ? À quelles fins ? Où vont-elles être stockées ? Nous pouvons également alerter sur la nécessité d'être vigilant quant aux données communiquées sur les réseaux sociaux. La limite de l'exercice étant qu'il faut que le consommateur aille lire l'information qui lui sera rendue disponible. Or, très souvent, il va être pressé d'obtenir un produit ou un service. En matière d'objet connecté,

il va être concentré sur le côté gadget ou branché de la chose, sans se poser la question des données personnelles. Ce n'est bien souvent qu'en cas de difficulté, qu'il revient vers les associations. C'est toute la limite de l'infirmation des consommateurs. Le site de service public de l'INC et celui de la CNIL restent des lieux ressource.

L'évolution de la réglementation tend-elle à renforcer la protection du consommateur ?

La réglementation européenne a procédé à une harmonisation et s'imposera fortement à tous puisque les états membres n'auront quasiment aucune liberté d'adaptation des textes. Les consommateurs citoyens européens seront protégés de la même façon. C'est une évolution, car ils auront davantage de droits à l'information, à l'exercice des droits d'accès, de rectification, limitation pour les professionnels du droit au profilage… La limite, c'est la manière dont va être mis en œuvre ce règlement européen qui change la donne, puisque nous passons d'un système global de déclaration de fichiers avec un contrôle à priori par les autorités de régulation à un système où les entreprises vont mettre en œuvre dès le départ la création de fichiers, etc. des règles visant à protéger les données personnelles avec un contrôle a posteriori par les autorités de contrôle.

Quels seront leurs moyens pour vérifier la bonne application des règles ? On peut dire que ça va dans le sens d'un renforcement des droits du consommateur, car vont être mis en place : un vrai consentement, un droit à l'oubli, à la mort numérique…

Au final, consommer va devenir plus simple ou plus compliqué ?

Les entreprises et leurs sous-traitants vont être responsables de la mise en œuvre du nouveau règlement européen puisqu'en cas de contrôle, c'est à elles de se justifier, de présenter leur registre de traitement des données, documenter tout ce qu'elles auront mis en œuvre pour permettre la sécurisation des données, etc. Mais le règlement renforçant également le droit à l'information des consommateurs, ceux-ci vont devoir — encore plus qu'avant – faire attention aux informations qui leur sont communiquées au départ et surtout avant de communiquer leur consentement à l'utilisation d'un objet connecté et à l'utilisation de leurs données personnelles. Ça va devenir un vrai métier.

#FSEtud-CGT

Vous pouvez retrouver les activités et les travaux de la Fédération CGT des Sociétés d'Etudes sur le Net !

Pour nous suivre, n'hésitez pas à consulter et à diffuser nos pages :

Notre fil d'actualité de la Revue de Presse Syndicale du Numérique (Numer'Action) sur Facebook : ***https://www.facebook.com/numeraction/?fref=ts***

La revue de presse Numer'Action en format pdf : ***http://www.soc-etudes.cgt.fr/nos-publications/numeraction***

Notre site Internet : ***http://www.soc-etudes.cgt.fr/***

La page de présentation des études du Colloque Impact du Numérique sur l'Emploi et le Travail du 6 décembre 2016 : ***http://www.soc-etudes.cgt.fr/vie-federale/etudes/2772-colloque-concernant-l-impact-du-numerique-sur-l-emploi-et-le-travail-documents-preparatoires***

Nos études fédérales : ***http://www.soc-etudes.cgt.fr/nos-publications/brochures***

Des liens sur les rapports, études et analyses concernant nos branches professionnelles :

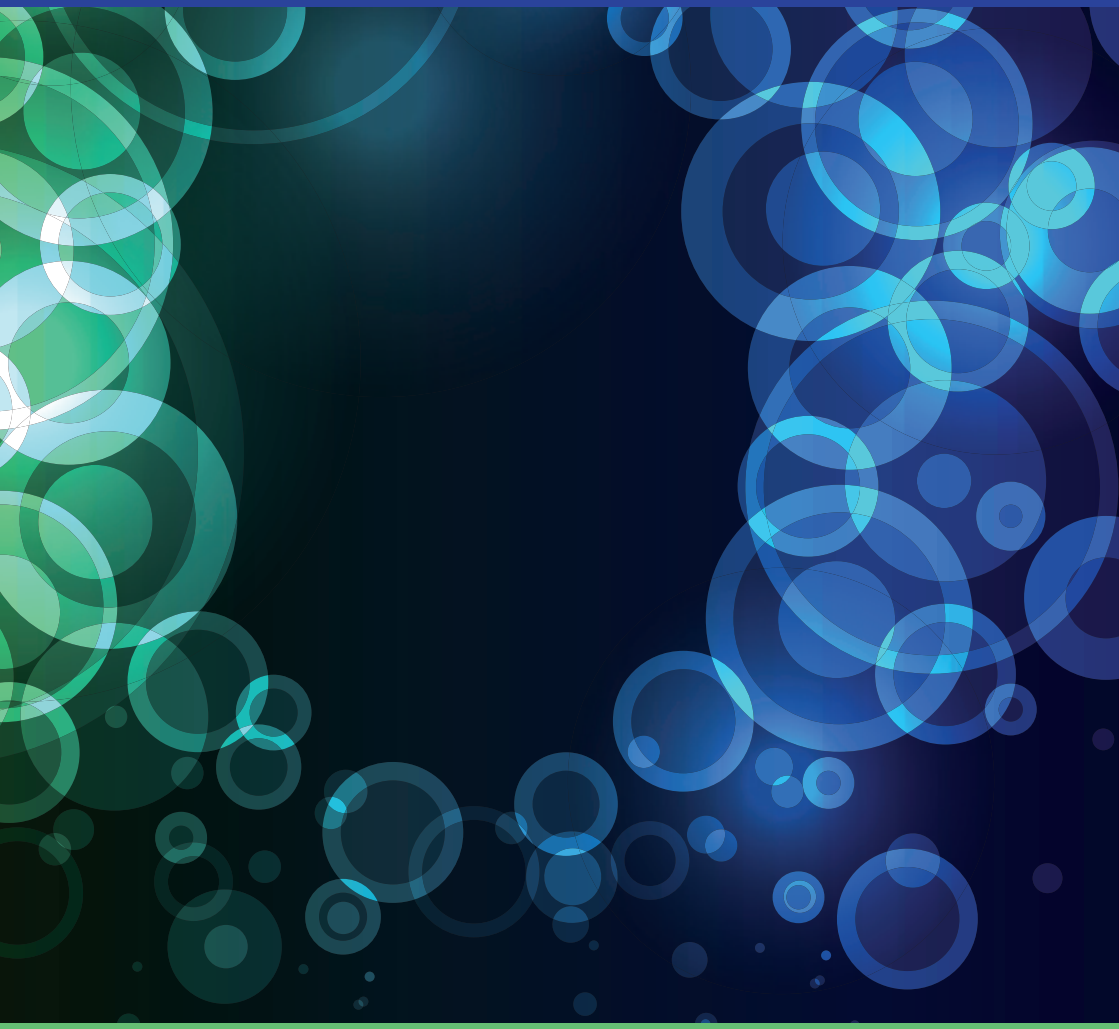
http://www.soc-etudes.cgt.fr/nos-branches/bureaux-d-etudes-techniques-de-conseil/325-rapports

http://www.soc-etudes.cgt.fr/nos-branches/bureaux-d-etudes-techniques-de-conseil/etudes

Notre page Twitter : ***https://twitter.com/fsetud***

Notre page Facebook : ***https://www.facebook.com/fsetud/?fref=ts***

la cgt Fédération sociétés d'études



Fédération CGT des Sociétés d'Etudes

263, rue de Paris - Case 421 - 93514 Montreuil - Cedex
Téléphone : 01 55 82 89 41 Fax : 01 55 82 89 42
E-mail : fsetud@cgt.fr - Site Internet : www.soc-etudes.cgt.fr