L'Union des Cadres et Ingénieurs Force Ouvrière

Protection des données personnelles, rgpd et relations de travail : une affaire trop sérieuse pour la laisser aux seules mains des employeurs

Les données en général, et les données personnelles en particulier (c'est-à-dire tout élément qui permet d'identifier, directement ou indirectement, une personne) sont au cœur de l'activité numérique. Produites en masse, elles atteignent aujourd'hui des volumes sans commune mesure et ce mouvement ne cesse de progresser notamment en raison de la puissance de calcul des processeurs informatiques, de la capacité de stockage et de la démultiplication des sources de données en raison notamment de la prolifération des capteurs et autres objets connectés.

De ce point de vue, le numérique invite tant à l'audace qu'à la vigilance. Audace pour que le numérique soit vecteur d'innovation et de progrès social. Vigilance pour qu'il ne devienne pas un cheval de Troie assiégeant nos libertés, nos vies privées, nos systèmes de garanties et de protection collectives.

ANALYSE ET PROSPECTIVE
MAI
2018
N°4

Éric Pérès
Secrétaire général

PROTECTION DES DONNÉES PERSONNELLES : DE LA LOI DU 6 JANVIER 1978 AU RGPD

Dès le 25 mai 2018, le RGPD, acte juridique européen, va encadrer la protection des données personnelles sur l'ensemble du territoire de l'Union. Contrairement à une directive, le règlement va s'imposer à tous ses Etats membres, quelle que soit leur législation nationale plus ou moins aboutie en la matière.

Ces changements nécessitent d'adapter la loi fondatrice du 6 janvier 1978, que le projet choisit symboliquement de ne pas abroger, tout en conservant son article 1er. Le projet de loi vise ainsi à modifier certains articles de la loi du 6 janvier 1978, soit pour les rendre compatibles avec le droit de l'Union (titre I), soit pour tirer parti des marges de manœuvre prévues par le Règlement. Ce projet de loi adopté définitivement par l'Assemblée nationale le 14 mai 2018 a donc pour objet la mise en conformité du droit national avec le « paquet européen de protection des données » adopté par le Parlement européen et le Conseil le 27 avril 2016 qui se compose :

- d'un Règlement (UE) 2016/679 (ci-après, « le Règlement ») relatif à la protection des personnes physiques à l'égard des données à caractère personnel, qui constitue le cadre général de la protection des données et est directement applicable à compter du 25 mai 2018 ;

- d'une Directive (UE) 2016/680 relative aux traitements mis en œuvre à des fins de prévention et de détection des infractions pénales, d'enquête et de poursuites en la matière ou d'exécution de sanctions pénales (ci-après « la Directive »).

Le recours devant le Conseil Constitutionnel sur le projet de loi de la part de soixante sénateurs le 16 mai ne permettra sans doute pas de garantir l'échéance du 25 mai pour l'application du RGPD en France; en effet sauf urgence, le Conseil constitutionnel dispose en principe d'un délai d'un mois pour statuer sur la dite saisine.

LES PRINCIPAUX CHANGEMENTS APPORTÉS PAR LE RGPD

Il est nécessaire de rappeler que le RGPD reprend le cadre actuellement applicable en le complétant avec des outils plus effectifs pour répondre aux réalités du monde numérique, de plus en plus globalisé. La plupart des principes de protection des données tels que prévus par le Règlement ne sont d'ailleurs pas nouveaux et sont déjà prévus par la Directive de 95 et la loi Informatique et Libertés du 6 janvier 1978 modifiée.

Un cadre juridique qui évolue autour du concept d' « accountability »

Le changement fondamental en termes de pratiques et d'état d'esprit réside dans le passage d'un contexte de conformité statique à une conformité dynamique avec le principe clé de « l'accountability » qu'introduit le règlement européen. Pour permettre aux entreprises de gérer leur conformité d'une façon dynamique et être en mesure de démontrer qu'elles respectent le RGPD conformément à ce principe « d'accountability » (logique de responsabilisation), les entreprises ou les administrations devront s'assurer notamment de la désignation d'un délégué à la protection des données (DPO), de la mise en œuvre des principes de « privacy by design et privacy by default », de la réalisation des études d'impact sur la vie privée (PIA), de la tenue d'un registre des traitements de données, de la notification de failles de violation des données dans un délai de 72h.

De nouvelles obligations pour les entreprises

Si la plupart des principes régissant le traitement de données à caractère personnel, posés par le législateur il y a près de 40 ans, restent toujours valables, le nouveau cadre juridique introduit un changement de paradigme majeur basé sur une logique de responsabilisation renforcée des acteurs, du responsables de traitement (entreprises, administrations, personnes morales) aux sous-traitants.

La logique de responsabilisation

Alors que la loi du 6 janvier 1978 reposait en grande partie sur une logique de « formalités préalables » (déclaration, autorisation, avis, normes simplifiées, etc.), le RGPD repose sur une logique de conformité continue, tout au long du cycle de vie de la donnée, dont les acteurs sont responsables, sous le contrôle et avec l'accompagnement de l'autorité de contrôle.

Le RGPD réduit donc la responsabilité administrative des responsables de traitements pour accroitre celle de leur responsabilité opérationnelle. L'idée est que la conformité doit être intégrée dans les processus opérationnels de tous les responsables de traitements, des entreprises, aux administrations par exemple. Ce principe de responsabilité est aussi celui qui doit promouvoir la protection des données dès la conception des traitements (privacy by design).

En d'autres termes, à l'exception des fichiers régaliens (police, justice), des traitements de données sensibles (biométrie, santé) qui disposent de dérogations nationales particulières au regard du RGPD, les entreprises en France comme dans toute l'Europe, n'auront plus à devoir s'acquitter des formalités préalables (autorisation, déclarations, avis..) avant la mise en œuvre d'un traitement de données personnelles auprès des différentes autorités de contrôle (la CNIL en France). Elles seront toutefois tenues à des obligations nouvelles pour démontrer qu'elles ont intégré cette logique de responsabilisation. Cette démarche doit les conduire à documenter l'ensemble des mesures et des politiques de protection des données.

Le délégué à la protection des données (DPO)

Afin de veiller à la conformité avec le RGPD, les responsables de traitement devront dans la plupart des cas désigner un DPO (Data Potecter Officer). Le DPO succède au CIL (Correspondant Informatique et Libertés) sauf que contrairement à ce dernier – facultatif – le DPO devient obligatoire pour une autorité publique ou un organisme public, à l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle, pour les entreprises de plus de 250 salariés et celles de moins de 250 salariés dont l'activité principale (les opérations clés nécessaires au responsable de traitement pour atteindre ses objectifs) implique soit un traitement de données personnelles qui du fait de leur nature et/ou de leurs finalités exigent un suivi régulier et systémique à grande échelle des personnes concernées, soit un traitement à grande échelles de données dites sensibles (santé, opinion politique, adhésion syndicale, orientation sexuelle, pratiques religieuses..).

Ainsi, les traitements de données nécessités par les fonctions support de l'entreprise, telles que, par exemple, la gestion RH ou la paie des employés, constituent des activités auxiliaires, qui n'exigent pas la désignation d'un DPO. Toutefois, le RGPD recommande, même pour les entreprises ne remplissant pas ces critères, de désigner un DPO.

Le DPO peut être interne ou externe à l'entreprise et peut également être mutualisé. Sa désignation doit s'accompagner de moyens lui assurant son indépendance. La fonction de DPO peut être occupée par un salarié d'une entreprise (juriste, responsable informatique, ancien CIL..). Celle-ci doit en revanche s'assurer que la

personne désignée soit notamment compétente dans le domaine de la législation et de la protection des données personnelles, et possède une bonne connaissance du secteur en question.

Le DPO doit en outre agir d'une manière indépendante et bénéficier d'une protection suffisante dans l'exercice de ses missions. Le RGPD prévoit ainsi que le délégué à la protection des données ne peut être relevé de ses fonctions ou pénalisé par l'employeur pour l'exercice de ses missions. L'employeur ne peut imposer des sanctions dans le cadre de l'exercice de sa fonction par le délégué à la protection des données.

Les missions du DPO sont :

- Informer et conseiller l'organisme ainsi que les salariés/agents sur les obligations qui lui incombent en vertu du RGPD et d'autres dispositions de l'Union ou de l'Etat membre concerné
- Contrôler le respect du RGPD, d'autres dispositions de l'UE ou de l'Etat membre concerné et des règles internes du responsable de traitement ou du sous-traitant (sensibilisation, formation du personnel, audits)
- Dispenser des conseils en ce qui concerne l'analyse d'impact relatif à la protection des données et vérifier son exécution
- Coopérer avec l'autorité de contrôle et faire office de point de contact pour les personnes concernées sur toute question en lien avec les traitements
- S'assurer de la bonne tenue de la documentation relative aux traitements

Le registre des activités de traitement

La tenue d'un registre des activités de traitement de données est une obligation qui s'étend à tous les responsables de traitement (entreprises, administration, associations, syndicats, ...) — avec ou sans DPO.

Le contenu du registre doit comprendre :

- Nom et coordonnées du responsable de traitement et du DPO
- Finalités du ou des traitements
- Catégories personnes concernées et les catégories de données
- Catégories de destinataires
- Dans la mesure du possible, les délais prévus pour l'effacement

Les entreprises de moins de 250 salariés en sont dispensées sauf si le ou les traitements de données à caractère personnel ne sont pas occasionnels, comportent des risques pour les droits et libertés des personnes et reposent sur des données sensibles (opinions politiques, adhésion syndicale, appartenance religieuse, orientations sexuelles, données de santé).

Une obligation s'étend aux sous-traitants qui devront tenir le registre des traitements qu'ils effectuent pour le compte de leurs clients commanditaires. Le contenu du registre du sous-traitant doit comporter :

- nom et coordonnées du ou des sous-traitants
- nom et coordonnées de chaque entreprise pour le compte de laquelle les sous-traitants ont une relation contractuelle
- catégories de traitements effectués pour le compte de chaque entreprise (responsable de traitement).
- transferts de données vers un pays tiers ou une organisation internationale
- dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles

Le registre des traitements doit être mis à disposition de la Cnil, qui pourra en solliciter la com-

munication dans le cadre de contrôles. En pratique, dans les entreprises, le service RH devra systématiquement en tenir un, dans la mesure où aucun des traitements RH mis en œuvre par le service RH ne peut être qualifié d'occasionnel et qu'il est également possible que des données sensibles soient collectées (santé par exemple).

Les études d'impact sur la vie privée (Privacy Impact Assessment ou PIA)

A la suite de la cartographie des traitements de données personnelles consignés dans le registre des traitements, l'entreprise comme tout responsable de traitement est dans l'obligation de réaliser une étude d'impact pour les traitements susceptibles d'engendrer un risque élevé pour les droits des personnes (cas d'une entreprise qui décide la mise en place d'un dispositif de vidéosurveillance ou de géolocalisation de ses salariés).

A l'issue de cette étude, si des risques résiduels d'atteinte aux droits des personnes – des salariés dans le cas d'espèce - demeurent, l'entreprise doit saisir l'autorité de contrôle de l'Etat membre pour trouver les mesures adaptées et être en conformité avec les principes du RGPD.

L'ensemble des CNIL's européennes (G29) ont définis neuf critères à prendre en compte pour identifier, de manière générale, un traitement de données personnelles qui nécessite le recours à une étude d'impact. Dès que deux critères au moins sont réunis, l'étude d'impact s'impose.

Appliquer au monde du travail, les critères à prendre en compte seraient :

- une évaluation ou une notation du salarié concernant par exemple le rendement au travail du salarié ou son état de santé, y compris l'établissement d'un profil ou d'une prédiction ;

- l'existence d'une décision automatisée à l'égard du salarié, produisant des effets juridiques ou similaires ;

- une surveillance systématique du salarié dans les locaux professionnels ou de son activité, y compris son poste de travail et son activité sur Internet ;

- la collecte de données sensibles ou données à caractère hautement personnel, telles que les données relatives à l'appartenance syndicale du salarié, les communications du salarié via son adresse e-mail non professionnelle, dont la confidentialité est protégée ;

- le traitement de données à large échelle (combinant le nombre de salariés concernés, la zone géographique, le volume de données et la durée du traitement) ;

- la combinaison ou le croisement de plusieurs jeux de données entre elles ;

- le traitement de données relatives à des personnes vulnérables - les salariés étant considérés comme des personnes vulnérables par le G29 en raison du lien de subordination du salarié avec son employeur ;

- l'utilisation innovante ou l'application de nouvelles solutions technologiques ou organisationnelles, par exemple, des systèmes de reconnaissance des empreintes digitales et de reconnaissance faciale des salariés pour améliorer le contrôle des accès physiques aux locaux professionnels ;

- le traitement qui empêche le salarié d'exercer un droit ou de bénéficier d'un service ou d'un contrat.

La notification obligatoire en cas de faille de sécurité des données

Dans le cas d'une faille de sécurité entrainant la violation de données personnelles (destruction accidentelle ou illégale des données, accès ou divulgation non autorisés, modification ou

altération des données personnelles, le responsable de traitement devra prévenir l'autorité de contrôle (la CNIL en France) dans un délai de 72 heures à partir de la prise de connaissance des faits.

Le responsable de traitement devra dans ce cas mettre tout en œuvre pour restaurer la sécurité des données. Il devra également informer en parallèle la ou les personnes concernées.

Des sanctions financières élevées en cas de manquement au RGPD

En contrepartie de la réduction voire de la suppression des formalités préalables auprès des autorités de contrôle (CNIL en France), ces dernières voient leurs pouvoirs de sanction renforcés.

Elles pourront sanctionner financièrement les responsables de traitement, une entreprise par exemple, d'un montant pouvant aller :

- jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires mondiale (le montant le plus élevé étant retenu) en cas de violation des exigences relatives aux principes essentiels du RGPD comme le droit d'accès, d'information, de rectification et selon la sensibilité des données ;

- jusqu'à 10 millions d'euros ou 2 % du chiffre d'affaires mondial (le montant le plus élevé étant retenu) pour d'autres infractions : non-tenue du registre, absence de DPO, non-respect du principe « privacy by design », par exemple.

Avec la révolution numérique, les entreprises qui sont amenées à collecter et à traiter d'importants volumes de données personnelles, celles de leurs clients tout comme celles de leurs salariés vont devoir donc faire preuve d'une plus grande vigilance dans la façon dont elles en assurent la collecte, le traitement et la protection.

Des nouveaux droits pour les personnes

Le RGPD renforce également les droits existants (droit d'accès, droit d'information, de rectification et d'opposition) en facilitant l'exercice de ceux-ci comme pour le consentement ou le droit à l'information, et lui en confère de nouveaux, comme le droit à la portabilité ou un droit à l'oubli propre pour les mineurs.

Ce droit à la portabilité est essentiel : il donne la possibilité à l'individu d'être indépendant de la plate-forme ou du prestataire auprès desquels il a développé une activité ou une existence en ligne. Il peut unilatéralement récupérer les données qu'il a fournies à un vendeur ou un réseau social, dans un format interopérable, et il peut les réutiliser comme bon lui semble.

Enfin, pour permettre une application uniforme et cohérente du règlement, le législateur européen a prévu un mécanisme de coopération renforcée entre les autorités de protection des données, qui devront adopter des décisions communes lorsque les traitements de données seront transnationaux, dans le cadre du mécanisme dit du « guichet unique ».

Les principes de base qui demeurent

FO-Cadres rappelle que tout traitement de données personnelles doit reposer sur six principes fondamentaux qu'il convient de garder à l'esprit :

Le principe de légalité : tout traitement de données personnelles doit reposer sur une base légale : le consentement, l'exécution d'un contrat, la sauvegarde de la vie humaine ou d'autrui, une disposition d'ordre légale, l'intérêt légitime.

Le principe de finalité : quel que soit le traitement ou le fichier mis en œuvre, celui -ci doit poursuivre un objectif clair, un objectif clairement identifié avant la mise en œuvre. Il convient alors

de s'assurer que cette finalité est déterminée de manière précise, explicite et légitime.

- L'entreprise doit réfléchir aux objectifs de l'outil et aux données dont elle a vraiment besoin au regard de la finalité définie et de déterminer si des données sensibles doivent être collectées. Par exemple l'utilisation d'un système de géolocalisation afin d'assurer le contrôle de la durée du travail des salariés n'est licite que lorsque ce contrôle ne peut pas être fait par un autre moyen, même moins efficaces (CE, 15 déc. 2017, n° 403776).

- Une entreprise qui utiliserait un traitement de données pour une finalité différente (profilage de salariés par exemple) de celle pour laquelle les données ont été initialement collectées initialement (sécurité par exemple) s'exposerait à des sanctions.

Le principe de proportionnalité : Les données qui sont collectées dans un cadre précis doivent en revanche «être adéquate, pertinentes et limitées à ce qui est nécessaire au regard de la ou des finalités». Ce principe poursuit celui de la minimisation, à savoir que l'on ne peut collecter que les données strictement nécessaire à la finalité poursuivie.

- Ainsi l'employeur ne peut pas collecter le numéro de sécurité sociale d'un candidat à l'embauche, ou encore des informations sur l'entourage familial ou l'état de santé. Le numéro de sécurité sociale (NIR) ne peut donc faire l'objet d'une collecte et d'un traitement qu'en vue du versement de la rémunération du salarié, pour permettre de calculer les cotisations versées aux organismes de protection sociale et de tenir le compte d'épargne salariale.

- Par exemple, dans le cadre d'un recrutement, et comme le rappelle le Code du travail, seules peuvent être collectées les informations permettant d'évaluer la capacité du candidat à occuper le poste. Il n'est a priori pas pertinent de collecter des données considérées comme sensibles, par exemple les opinions politiques ou l'appartenance syndicale des candidats.

Le principe de qualité et de durée : les données doivent être « exactes et si nécessaire tenues à jour » et conservées pendant une durée qui ne peut excéder la durée nécessaire à la poursuite de la finalité initiale et pour laquelle elles sont été collectées*.

- L'entreprise doit supprimer de manière définitive les données à l'issue de la durée de conservation recommandée au regard des finalités pour lesquelles elles sont traitées. Les données peuvent être conservées pour une durée plus longue en mode archivage et non en mode actif, avec limitation des personnes habilitées à y accéder.

Le principe de sécurité : les données doivent être protégées dans le respect de l'art en veillant au stockage, physique et logique, tout comme au politique d'habilitation pour les accès dédiés.

Le principe de loyauté : un traitement des données personnelles ne peut être mis en œuvre sans une information préalable.

- Aucune information concernant un candidat à un emploi ne peut être collectée par un dispositif qui n'a pas été porté préalablement à sa connaissance.

- L'entreprise devra gérer les demandes d'accès, de rectification et de suppression émanant des salariés.

- Il faudra alors par exemple veiller à ce que le service RH rédige convenablement une notice d'information à l'intention des candidats au recrutement ou des salariés embauchés, incluant les informations suivantes lorsque

la collecte est effectuée directement auprès du candidat ou du salarié (lors de son recrutement par exemple).

PROTECTION DES DONNÉES PERSONNELLES ET RGPD : UN ENJEU SYNDICAL

Le RGPD met en place une nouvelle grammaire du traitement des données au sein des entreprises comme des administrations. C'est une toute nouvelle façon de construire de la valeur ajoutée pour de nombreuses entreprises. Mais c'est aussi une opportunité pour renforcer une différenciation compétitive hors coût, basée sur le respect des droits des personnes et la protection de la vie privée.

Dans le capitalisme numérique, l'objectif premier n'est plus l'argent, mais l'accumulation du plus grand nombre de données et tout particulièrement des données personnelles. Pour Facebook, cette fonction consiste à maximiser l'engagement de ses usagers, pour Google, c'est l'adéquation des résultats de recherche aux attentes des utilisateurs, pour Amazon les ventes, etc. Dans les relations de travail, les traitements de données personnelles répondent à des obligations RH traditionnelles (paie, congés...) mais dans certains ils peuvent poursuivre des finalités en matière de gestion des compétences et des recrutements qui comportent, en l'absence de régulation et de contrôle, des risques réels et sérieux de discrimination, d'exclusion du bénéficie d'un droit, de contrôles intrusifs et abusifs des salariés. Sans compter les cas où les traitements de données personnelles des salariés peuvent être collectés dans le but d'accroitre leur surveillance, leur productivité au mépris de leur santé, le contrôle de leurs déplacements, d'établir des évaluations en vue de licenciements programmés, de détecter des salariés dits « toxiques », voire de renforcer la sélection par le profilage sur la base de données extra-professionnelles.

Dans tous les cas les exemples de questions RGPD dans le cadre des relations de travail sont nombreux:

Recrutement : l'entreprise a-t-elle respecté ses obligations vis-à-vis des candidats en ne traitant que des données strictement professionnels ? Ses contrats avec les cabinets de recrutements sont-ils conformes aux exigences du RGPD ? L'entreprise a-t-elle informé les candidats, les salariés et les IRP de l'utilisation d'outil dit « d'intelligence artificielle » dans le recrutement ? L'entreprise a-t-elle recours à la collecte de données sur les réseaux sociaux ?

Embauche : L'entreprise respecte-t-elle dans la collecte des données du salarié lors de l'embauche les principes du RGPD notamment celui de la minimisation des données (principe de proportionnalité) ? L'entreprise informe-t-elle correctement les salariés sur les traitements de données personnelles les concernant lors de l'embauche (nature des données, finalités, destinataire, durée de conservation, droit d'accès...) ?

Relation au travail : L'entreprise informe-t-elle correctement les salariés et les IRP sur les traitements de données personnelles qu'elle met en œuvre (géolocalisation, vidéosurveillance, vidéoprotection, algorithmes de gestion de talents, utilisation des outils numériques, management algorithmique...) ? Ces traitements sont-ils respectueux de la vie privée des salariés ? L'entreprise a-t-elle respecté les exigences du RGPD en matière de sécurité des données lors d'élections professionnelles ? A-t-elle effectué une étude d'impact dans le cas d'une mise en œuvre d'un dispositif de badgeage ou de géolocalisation ? Les traitements de données collectées et traitées dans le cadre de la politique de rémunération et d'avantages sociaux sont-ils respectueux de la vie privée des salariés ? Les formations et

le déroulement de carrières donnent-ils lieu à des traitements de données ?

L'enjeu de la protection des données personnelles des salariés dans le cadre du RGPD doit être pour notre organisation l'occasion de réaffirmer notre combat pour la protection de la vie privée des salariés et poursuivre la lutte contre toute forme de surveillances abusives, de géolocalisations liberticides, de fichage et d'évaluation arbitraire et intrusive, de discrimination des salariés dans le cadre des relations de travail. Cet enjeu doit être saisi comme un levier d'action syndicale pour veiller au respect des droits des salariés.

CONCLUSION

Le développement du tout-technologique en matière de sécurité ne doit pas faire oublier les risques de dérives inhérents aux systèmes de collecte et de traitements de données à caractère personnel. Des salariés filmés à leur insu dans leur vestiaire, des empreintes digitales collectées et stockées en douce, des données personnelles revendues au plus offrant. Lorsqu'il est question de surveillance physique, le fantasme du Big Brother omniscient manipulant les salariés réduits au rang d'objet, n'est jamais très loin. En témoignent les dispositifs de cybersurveillance (caméras, puces RFID, géolocalisation..) qui sont de plus en plus intrusifs grâce à l'évolution des technologies et, par voie de conséquence, plus fréquemment susceptibles de violer le respect de la vie privée des personnes surveillées.

Le développement exponentiel des mécanismes de traçage est réel. Les technologies peuvent s'attaquer ainsi à l'intimité des salariés, à leurs données personnelles, à celles de leur famille. Il est vrai que les technologies en général et les technologies numériques en particulier sont ambivalentes. Elles peuvent offrir de réelles potentialités dans de nombreux domaines (santé, aéronautique, énergie, construction, mobilité...) et concourir par le progrès technologique au progrès social et humain. Mais a contrario, sans cadre légal, sans régulation, ni contrôle et respect des droits des personnes, ces mêmes technologies peuvent servir des finalités attentatoires aux libertés fondamentales.

Au sein des entreprises et des administrations, une solution doit s'imposer : le respect des droits des salariés et des agents en matière de respect de la vie privée, celui du respect du droit à l'information sur l'utilisation dans les entreprises et les administrations de traitements de données personnelles et le respect du dialogue social pour que l'utilisation du numérique ne soit pas un processus banalisé. L'utilisation du numérique dans les relations de travail est une affaire trop sérieuse pour la laisser aux seules mains des DSI et des DRH. Cela oblige donc à communiquer autour de la mise en place de ces systèmes, et de se saisir de ces questions dans le cadre des instances du dialogue social tout en rappelant que les

libertés fondamentales et le respect de la vie privée ne se marchandent ni ne se négocient.

Dans une société soumise à d'innombrables questions sur sa capacité à faire face à l'imprévisible l'absence de questionnement critique sur ces évolutions technologiques (Big data, algorithmes, intelligence artificielle) serait préjudiciable à l'État de droit. Il est donc indispensable de placer les questions d'innovation et de protection au cœur de nos réflexions et revendications syndicales. Le sens critique syndical doit prévaloir pour comprendre ces transformations numériques en cours et peser sur elles pour assurer la continuité des protections individuelles et collectives des salariés. Un travail que notre organisation FO syndicale n'a jamais sous-estimé, tant les impacts du numérique sur la vie des salariés sont réels.

Dans cette perspective FO-Cadres poursuivra son travail d'information et de formation auprès des cadres et ingénieurs FO et de l'ensemble des camarades, pour faire de la question de la protection des données personnelles un levier d'action pour le développement syndical. Elle reviendra en détail sur les aspects particulier du lien entre RGPD et les relations de travail. Dès la rentrée, FO-Cadres mettra à disposition des cadres et ingénieurs FO une formation dédiée à l'enjeu et à la maitrise des outils RGPD dans le domaine RH. Elle mettra enfin son expertise à la disposition de notre organisation confédérale dans le cadre de ses action en lien avec le numérique.

FO-CADRES — BUSINESS CENTER OPÉRA - 5e ÉTAGE - 3, AVENUE DE L'OPÉRA - 75001 PARIS — TÉL. 01 47 42 39 69 - CONTACT@FO-CADRES.FR