L’immatériel dans les relations économiques

Sources : economie.gouv.fr / jurifiable.com / legifrance

III. Le règlement général sur la protection des données (RGPD), mode d’emploi

A. Le RGPD, qu’est-ce que c’est ?

Le règlement général de protection des données (RGPD) est un texte réglementaire européen qui encadre le traitement des données de manière égalitaire sur tout le territoire de l’Union Européenne. Il est entré en application le 25 mai 2018.

Le RGPD s’inscrit dans la continuité de la Loi française Informatique et Libertés de 1978 établissant des règles sur la collecte et l’utilisation des données sur le territoire français. Il a été conçu autour de 3 objectifs :

- **renforcer les droits des personnes**
- **responsabiliser les acteurs traitant des données**
- **crédibiliser la régulation** grâce à une coopération renforcée entre les autorités de protection des données.

B. Données personnelles : de quoi parle-t-on ?

Une **donnée personnelle** est décrite par la CNIL comme « toute information se rapportant à une personne physique identifiée ou identifiable ». Il existe 2 types d’identifications :

- identification directe (nom, prénom etc.)
- identification indirecte (identifiant, numéro etc.).

Lorsqu’une opération ou un ensemble d’opérations portant sur des données personnelles sont effectuées, on considère qu’il s’agit de **traitement de données personnelles**. La CNIL donne les actions suivantes à titre d’exemple du traitement des données :

- tenue d’un fichier de ses clients
- collecte de coordonnées de prospects via un questionnaire
- mise à jour d’un fichier de fournisseurs

La création et le traitement de données personnelles (numéro d'identifiant, nom, adresse, numéro de téléphone, photo, adresse IP notamment) sont soumis à des obligations destinées à protéger la vie privée et les libertés individuelles. De nouvelles obligations sont à la charge des entreprises, administrations, collectivités, associations ou autres organismes permettant d'accorder des droits plus étendus à leurs clients / usagers. Le régime des sanctions évolue également.

1. Qu'est-ce qu'une donnée personnelle ?

Il s'agit de toutes informations se rapportant à une personne physique identifiée ou identifiable, directement ou non, grâce à un identifiant ou à un ou plusieurs éléments propres à son identité.

Il peut s'agir par exemple d'un nom, d'un prénom, d'une adresse électronique, d'une localisation, d'un numéro de carte d'identité, d'une adresse IP, d'une photo, d'un profil social ou culturel.

Les règles s'appliquent lorsqu'elles sont utilisées, conservées ou collectées numériquement ou sur papier.

2. Qui est concerné ?

Le règlement s'applique à tous les traitements de données à caractère personnel, sauf exceptions (les fichiers de sécurité restent régis par les États et les traitements en matière pénale par exemple).

Il concerne :

- les responsables de traitement (entreprises, administrations, associations ou autres organismes) et leurs sous-traitants (hébergeurs, intégrateurs de logiciels, agences de communication entre autres) établis dans l'Union européenne (UE), quel que soit le lieu de traitement des données.

- les responsables de traitement et leurs sous-traitants établis hors de l'UE, quand ils mettent en œuvre des traitements visant à fournir des biens ou des services à des résidents européens ou lorsqu'ils les ciblent avec des techniques algorithmiques (technique du profilage).

En pratique, le règlement s'applique donc à chaque fois qu'un résident européen, quelle que soit sa nationalité, est directement visé par un traitement de données, y compris par internet ou par le biais d'objets connectés (appareils domotiques, objets mesurant l'activité physique par exemple).

C. Droit des personnes

1. Consentement renforcé et transparence

Les données personnelles doivent être :

- traitées de manière licite, loyale et transparente et collectées pour des finalités déterminées ;
- explicites et légitimes ;
- adéquates, pertinentes et limitées aux finalités du traitement ;
- exactes et tenues à jour ;
- conservées de façon temporaire et sécurisée.

Les clients ont un droit d'accès à leurs données et peuvent les rectifier et s'opposer à leur utilisation.

Sur demande, l'entreprise qui détient des données personnelles doit informer la personne concernée avec les éléments suivants :

- identité du responsable du fichier ;
- finalité du traitement des données ;
- caractère obligatoire ou facultatif des réponses ;
- droits d'accès, de rectification, d'interrogation et d'opposition ;
- les obligations induites par les transmissions des données.

2. Droit à la portabilité des données

Toute personne peut récupérer, sous une forme réutilisable, les données qu'elle a fournies et les transférer ensuite à un tiers (réseau social par exemple).

La portabilité concerne uniquement les données recueillies dans le cadre d'un contrat ou d'un consentement.

3. Droit à l'oubli

Toute personne a droit à l'effacement de ses données et au déréférencement (droit de demander à un moteur de recherche de supprimer certains résultats associés à ses noms et prénoms).

4. Droit à notification

En cas de violation de la sécurité des données comportant un risque élevé pour les personnes, le responsable du traitement doit les avertir rapidement, sauf dans certaines situations (données déjà chiffrées par exemple). Il doit également le notifier à la Cnil dans les 72 heures.

5. Droit à réparation du dommage matériel ou moral

Toute personne qui a subi un dommage matériel ou moral du fait de la violation du règlement européen peut obtenir du responsable du traitement (ou du sous-traitant) la réparation de son préjudice.

6. Action de groupe

Toute personne peut mandater une association ou un organisme actif dans le domaine de la protection des données pour faire une réclamation ou un recours et obtenir réparation en cas de violation de ses données. Obligations des entreprises, administrations, collectivités, associations

D. Obligation générale de sécurité et de confidentialité

Le responsable du traitement des données doit mettre en œuvre les mesures de sécurité des locaux et des systèmes d'information pour empêcher que les fichiers soient déformés, endommagés ou que des tiers non autorisés y aient accès.

Il doit prendre toutes les mesures nécessaires au respect de la protection des données personnelles dès la conception du produit ou du service.

Ainsi, il est tenu de limiter la quantité de données traitée dès le départ (principe dit de « minimisation ») et doit démontrer cette conformité à tout moment.

L'accès aux données est réservé uniquement aux personnes désignées ou à des tiers qui détiennent une autorisation spéciale et ponctuelle (service des impôts par exemple.).

Le responsable des données doit fixer une durée raisonnable de conservation des informations personnelles.

Les obligations déclaratives sont toutes supprimées, sauf exceptions prévues par le droit national (certains traitements dans le secteur de la santé, ou de la sécurité publique mis en œuvre pour le compte de l'État).

1. Obligation d'information

L'entreprise qui détient des données personnelles doit informer la personne concernée de :

- l'identité du responsable du fichier ;
- la finalité du traitement des données ;
- le caractère obligatoire ou facultatif des réponses ;
- les droits d'accès, de rectification, d'interrogation et d'opposition ; • les transmissions des données.

L'exploitant de données personnelles (un commerçant en ligne par exemple) doit respecter certaines obligations, et notamment :

- recueillir l'accord des clients ;
- informer les clients de leur droit d'accès, de modification et de suppression des informations collectées ;
- veiller à la sécurité des systèmes d'information ;
- assurer la confidentialité des données ;
- indiquer une durée de conservation des données.

L'objectif de la collecte d'informations doit être précis et les données en accord avec cette finalité.

À savoir : la majorité numérique, l'âge à partir duquel un mineur peut consentir seul au traitement de ses données personnelles pour utiliser un service sur internet (les réseaux sociaux par exemple), est fixée à 15 ans. L'autorisation des parents est nécessaire avant cet âge. L'information relative au traitement de données du mineur doit être rédigée en termes clairs et simples.

2. Analyse d'impact en cas de risque élevé pour les droits et libertés des personnes

Pour les traitements de données présentant un risque élevé pour les droits et libertés des personnes, le responsable du traitement doit mener une analyse d'impact sur la vie privée (PIA) pour évaluer , en particulier, l'origine, la nature, la particularité et la gravité de ce risque.

Cette étude doit être présentée à la Cnil si elle n'a pas permis de diminuer suffisamment le risque pour le rendre acceptable.

Les données concernées doivent porter sur :

- les informations sensibles (origine, opinions politiques, religieuses, syndicales), biométriques ou génétiques notamment ;
- l' évaluation des personnes (profilage par exemple) ;
- les fichiers ayant une finalité particulière (études statistiques de l'Insee, traitements de recherche médicale par exemple) ;
- les transferts de données hors de l'Union européenne.

À noter : les transferts de données hors de l'UE ne sont plus interdits mais ils doivent respecter plusieurs conditions, notamment que le pays tiers présente un niveau de protection adapté, selon la Commission européenne. Une

autorisation de la Cnil est nécessaire si des clauses contractuelles diffèrent des clauses de la Commission européenne. Les données transférées restent soumises au droit de l'UE non seulement pour leur transfert, mais aussi pour tout traitement / transfert ultérieur.

3. Délégué à la protection des données (DPD ou DPO)

Le responsable de traitement et le sous-traitant doivent désigner un délégué à la protection des données :

- si leur activité fait partie du secteur public ;
- si leur activité principale amène un suivi régulier et systématique de personnes à grande échelle ;
- si leur activité principale amène le traitement à grande échelle de données sensibles ou relatives à des condamnations pénales et infractions.

Le délégué est chargé :

- d'informer et de conseiller le responsable de traitement (ou le sous-traitant) et ses employés ;
- de contrôler le respect du règlement européen et du droit français en matière de protection des données ;
- de conseiller l'organisme sur la réalisation d'une analyse d'impact et d'en vérifier l'exécution ;
- de coopérer avec l'autorité de contrôle et d'être son contact.

Le délégué à la protection des données doit avoir les qualités et compétences suivantes :

- communiquer efficacement et exercer ses fonctions en toute indépendance (ne pas avoir de de conflit d'intérêts avec ses autres missions) ;
- une expertise en matière de législations et pratiques (protection des données), acquise notamment par une formation continue ;
- une bonne connaissance du secteur d'activité et de l'organisation de l'organisme (opérations de traitement, systèmes d'information et besoins de l'organisme en matière de protection et de sécurité des données) ;
- une position efficace en interne pour faire un rapport au niveau le plus élevé de l'organisme ;
- animer un réseau de relais au sein des filiales d'un groupe par exemple et/ou une équipe d'experts en interne (expert informatique, juriste, expert en communication, traducteur par exemple).

Le délégué peut être une personne issue du domaine technique, juridique ou autre.

Indépendance du DPD

Selon l'Article 38 du RGPD (Règlement Général sur la Protection des Données), le DPD doit pouvoir exercer ses fonctions en toute indépendance et ne doit pas recevoir d'instructions directes concernant l'exercice de celles-ci. L'indépendance est cruciale pour permettre au DPD de superviser la conformité aux lois sur la protection des données sans pression ni influence externe.

Conflit d'Intérêts

Le rôle du DPD est de surveiller l'adhérence de l'organisation aux régulations de protection des données, ce qui peut inclure l'évaluation des risques associés aux nouvelles technologies ou pratiques IT que le DSI pourrait vouloir mettre en œuvre. Si le DPD dépend du DSI, cela pourrait créer un conflit d'intérêts, car il pourrait être moins enclin à signaler ou agir contre des pratiques qui pourraient être avantageuses pour le département IT mais risquées du point de vue de la protection des données.

Recommandations pour l'Organisation

Pour éviter ces conflits et garantir l'efficacité du rôle du DPD, il est généralement recommandé que le DPD rapporte à un niveau de direction capable de prendre des décisions transversales affectant l'ensemble de l'organisation, tel que le directeur général ou le conseil d'administration. Cela aide à garantir que le DPD ait l'autorité et les ressources nécessaires pour mener à bien ses missions et pour intervenir efficacement dans toutes les divisions de l'organisation.

4. Autres obligations

Tous les organismes (publics comme privés) qui traitent des données personnelles ont l'obligation de tenir un registre de l'ensemble des traitements.

Toutefois les entreprises de moins de 250 salariés doivent seulement inscrire au registre :

- les traitements non occasionnels ;
- les traitements susceptibles de comporter un risque pour les droits et libertés des personnes ;
- les traitements qui portent sur des données sensibles.

Sanctions administratives
En cas de violation du règlement, la Cnil peut prononcer des amendes administratives qui peuvent atteindre, selon la catégorie du manquement, 2 % à 4 % du chiffre d'affaires annuel mondial de l'exercice précédent.

IV. Entreprise et vie privée : quels sont les droits de l'employeur et du salarié ?

A. Utilisation des TIC, droit à la déconnexion, données personnelles, outils de contrôle…

Selon l'article 9 du Code civil, chacun a droit au **respect de sa vie privée**, y compris le salarié sur son lieu de travail et pendant son temps de travail.
La Cour de cassation a d'ailleurs consacré la notion de **vie personnelle du salarié**, notion plus large que celle de la vie privée, par opposition à la **vie professionnelle.**
Ainsi, l'employeur ne peut, en principe, s'immiscer dans la vie privée de ses salariés ni les sanctionner pour un fait relevant de leur vie personnelle. Toutefois, dans la relation qui lie l'employeur et le salarié, ce droit peut subir **quelques restrictions** lorsqu'elles sont nécessaires et proportionnées au but poursuivi. C'est la **jurisprudence** qui joue ici un rôle fondamental pour déterminer la limite entre les droits du salarié et ceux de l'employeur…
Vidéosurveillance, géolocalisation, droit à la déconnexion, utilisation des données personnelles, utilisation d'internet, etc., nous allons exposer ci-dessous les **principales règles qui encadrent les limites entre l'entreprise et la vie privée du salarié.**

B. L'employeur a t-il le droit de surveiller les salariés dans l'entreprise ?

Le principe général à respecter en matière de surveillance des salariés au travail est celui de **la transparence.** Ainsi, une **information préalable du salarié** est nécessaire (C. trav. L1224-4) et le **règlement intérieur** doit mentionner le système de surveillance (C. trav. L3111-2 et L1321-3).
De plus, l'employeur est tenu de **consulter les représentants du personnel** avant la mise en place de la surveillance (C. trav. art. L2323-32) et les moyens mis en œuvre doivent être **justifiés et proportionnés** au but recherché (C. trav. art. L 1121-1).
Enfin, il faut savoir que tout système de surveillance ou d'analyse des discussions des salariés (vidéosurveillance, connexions internet…) doit faire l'objet d'une **déclaration à la Cnil** (Commission national de l'informatique et des Libertés) ou bien d'une inscription sur le registre du correspondant informatique et liberté (CIL) dans son entreprise.
La chambre sociale de la Cour de cassation estime ainsi que si le contrôle s'effectue sur le lieu du travail à l'insu des salariés, **les enregistrements vidéo** effectués constituent un **mode de preuve illicite** (Cass. soc. 10 janvier 2012 n°1023.482). En revanche, la chambre criminelle de la Cour de cassation estime quant à elle que ces enregistrements **peuvent être retenus comme preuve de vol**dans la caisse par un employé (Cass. crim. 6 avril 1994 n°93-82.717). On peut donc en conclure que les enregistrements vidéo à l'insu d'un salarié ne sont pas retenus aux prud'hommes mais peuvent être retenus devant le Tribunal correctionnel.
A contrario, **si les salariés sont avertis de la surveillance effectuée, celle-ci est alors autorisée.** Il en est ainsi pour des salariés avertis que leurs conversations téléphoniques pourraient être écoutées. Les écoutes réalisées constituent d'ailleurs un **mode de preuve recevable** pour fonder un licenciement (Cass. soc. 14 mars 2000 n°98-42.090).
Quelques exceptions… L'obligation d'informer préalablement les salariés ne concerne pas les systèmes de vidéosurveillance dans des locaux où les salariés ne travaillent pas. Il en est notamment ainsi de la vidéosurveillance mise en place dans un entrepôt de marchandises. De même, si le système de vidéosurveillance a pour but de prévenir le risque d'intrusion dans les locaux d'une entreprise, il n'est alors pas nécessaire que les salariés soient informés de manière personnelle. Il en est notamment ainsi lorsque les caméras sont dirigées vers la porte de l'agence et non vers le poste de travail (CA de Dijon du 29 novembre 20122, n° 11-01.139).
Rappelons enfin que le salarié, même averti de la mise en place du système de **géolocalisation**, doit pouvoir la désactiver dès lors qu'il utilise le véhicule dans le cadre de sa vie privé (CA de Bordeaux du 25 novembre 2008 n° 0705.964).

C. L'employeur a t-il accès aux documents détenus par le salarié dans l'entreprise : données informatiques, clé USB, dossiers, mails, etc. ?

En principe, **le matériel fourni par l'entreprise au salarié a un caractère professionnel**. L'employeur peut y avoir accès sans que la présence du salarié soit nécessaire. Il en est ainsi des dossiers et fichiers informatiques qui se trouvent sur l'ordinateur mis à disposition par l'entreprise, de la clé USB, de la correspondance ou des mails reçus par le salarié. Toutefois, l'employeur ne peut pas consulter ces documents si ceux-ci sont **identifiés comme « personnel » « confidentiel » ou « privé ».** Notons que cette interdiction est également valable pour des mails reçus par le salarié alors même que l'employeur avait interdit une utilisation non professionnelle de l'ordinateur. Il existe toutefois des cas où **l'employeur est autorisé à consulter des documents personnels :**

- si la consultation s'effectue en présence du salarié ;
- en cas de danger menaçant l'entreprise, si le contrôle des fichiers ou courriers électroniques est nécessaire (par exemple, risque de piratage de données, acte de terrorisme, etc.) ;
- si une mesure d'instruction est mise en place (C. proc. civ., art. 145).

Par contre, l'employeur ne viole pas le secret des correspondances **s'il ouvre un pli ne contenant aucune mention sur son caractère personnel** (Cass. soc. 18 mai 2007, n° 05-40.803).

Et si l'employeur a le droit de consulter les **documents non signalés comme personnels**, il ne peut en revanche les utiliser contre le salarié dans une procédure judiciaire s'ils relèvent de sa vie privée. Ainsi, l'employeur ne peut utiliser des mails que le salarié a échangés avec sa petite amie pour prouver sa volonté de démissionner ou la réalité de ses horaires de travail (Cass. soc. 18 octobre 2011, n° 10-25706). Au contraire, **il peut se servir d'un mail non identifié comme privé,** adressé à un autre salarié de l'entreprise, dont le contenu est en rapport avec l'activité professionnelle (Cass. soc. 2 février 2011, n° 09-72450).

D. Quelles sont les règles relatives à l'utilisation d'internet dans l'entreprise ?

1. Quelles sont les limites imposées au salarié ?

En principe, le salarié n'a **pas le droit d'utiliser internet à des fins personnelles** durant ses heures de travail. Toutefois, il existe une tolérance… qui s'applique jusqu'à l'abus !

Ainsi, un salarié qui utilise la connexion Internet de l'entreprise, pour des raisons personnelles pendant sa pause déjeuner, ne peut pas être licencié dans la mesure où il ne commet pas d'abus. En revanche, un salarié qui reste connecté toute la journée pour des raisons privées sans effectuer son travail s'expose logiquement un risque de licenciement !

Par ailleurs, **la faute peut résulter de la nature des sites internet consultés**, notamment les sites pornographiques. L'usage personnel excessif constitue donc **une faute grave**. Il en est notamment ainsi dans une affaire où un salarié avait « surfé » sur des sites sans rapport avec son travail (sexe, humour, politique), téléchargé et adressé par mail à des collègues des vidéos, des textes et des images alors que le règlement de l'entreprise l'interdisait (Cass. soc. 18 décembre 2013, n° 12-17.832).

De même, peut être sanctionnée la salariée qui reste connectée, à des fins personnelles, 41 heures en un mois (Cass. soc. 18 mars 2009, n° 07-44.247). Idem pour la salariée qui avait échangé avec un autre salarié à titre privé plus de 2 000 mails en 12 mois et qui lui avait même adressé des images personnelles pour les imprimer avec le matériel de l'entreprise (CA de Rennes du 6 décembre 2013, n° 11-07.157).

Au contraire, **passer une heure par semaine sur internet à des fins personnelles ne constitue pas un usage abusif.**

2. Quelles sont les limites imposées à l'employeur ?

S'il existe des limites à l'utilisation d'internet par le salarié durant ses heures de travail, il existe également une limite qui s'impose à l'employeur. En effet, **l'employeur ne doit pas pouvoir empiéter, comme bon lui semble, dans la sphère privée du salarié**. Cette limite se traduit par ce que l'on appelle le **droit, pour le salarié, à la déconnexion.**

En effet, la loi Travail du 8 août 2016 accorde au salarié qui travaille dans une entreprise de plus de 50 salariés un droit à la déconnexion. Ce droit permet au salarié de ne plus être collé à son smartphone et soumis aux multiples mails et sms professionnels même après le travail.

Depuis le 1er janvier 2017, l'employeur a **deux possibilités pour mettre en pratique ce droit** : il peut parvenir à **un accord collectif** ou, s'il n'y parvient pas, **établir une charte**. Cette charte, rédigée après avis du comité d'entreprise ou des délégués du personnel, doit définir les **modalités d'une utilisation saine des outils numériques** dans l'entreprise. Le droit à la déconnexion prévoit ainsi de respecter, pour chaque salarié, **les temps de repos,** à savoir 11h minimum par jour et 35h par semaine.

Sachez qu'il n'existe **pas de sanction en cas d'absence de charte.** En revanche, l'employeur a l'obligation de négocier. S'il refuse, il est sanctionné pénalement pas un an d'emprisonnement et 3750 euros d'amende (C. trav. art. L2242-8).

L'employeur peut-il se servir de faits relevant de la vie privée du salarié pour le sanctionner ?

En principe, **un fait tiré de la vie privée ne peut justifier le licenciement d'un salarié**, sauf s'il constitue un manquement du salarié à une obligation découlant de son contrat de travail ou s'il a un impact sur la vie de l'entreprise. **Pour pouvoir sanctionner un salarié, la faute commise dans le cadre de la vie privée doit être au moins en lien avec les obligations du contrat de travail**. Le premier exemple qui vient à l'esprit est sans doute celui du chauffeur qui perd son permis de conduire pour conduite en état d'ivresse en dehors de ses horaires de travail.

Dans la même logique, le licenciement d'un membre du personnel naviguant qui avait consommé de la drogue lors d'une escale entre deux vols et qui se trouvait donc sous son influence pendant l'exercice de ses fonctions a donc été considéré comme justifié (Cass. soc. 27 mars 2012, n° 10-19915). De même, le licenciement d'un salarié incarcéré est justifié si l'employeur établit que l'absence du salarié désorganise ou perturbe le fonctionnement de l'entreprise. **Il est important de préciser que même si l'employeur est autorisé à licencier le salarié, ce licenciement ne peut être motivé par une faute.** Il s'agit en effet d'un licenciement pour motif personnel, non fautif, ouvrant droit à toutes les indemnités de rupture de contrat (indemnité de congés payés, indemnité légale ou conventionnelle de licenciement, éventuellement indemnité de préavis).

Toutefois, **les faits de la vie personnelle peuvent être sanctionnés par l'employeur s'ils ont un lien avec l'activité professionnelle et qu'ils causent un trouble à l'entreprise**. Il en est notamment ainsi d'un salarié licencié pour faute grave pour avoir blessé un autre salarié qui était venu récupérer le véhicule de l'entreprise à son domicile (Cass. soc. 6 février 2002, n° 99-45.418). On peut également soulever le cas d'une salariée licenciée après avoir tenu des propos dénigrants et insultants sur Facebook avec un ancien responsable de son entreprise. Ce licenciement pour faute a été jugé bien-fondé par les juges (CA Besançon 15 novembre 2011 n°10-02.642).