Sous la coordination scientifique de
Grégoire Loiseau
Professeur à l'école de droit de la Sorbonne (Paris 1)

LE DROIT DES DONNÉES À CARACTÈRE PERSONNEL DANS LES RELATIONS DE TRAVAIL

BJT202t1

Le droit des données à caractère personnel, conçu pour s'appliquer à tout traitement de données se rapportant à une personne physique, s'accommode progressivement aux spécificités des relations de travail. Les entreprises ont développé une pratique pour l'application des règles prescrites par le règlement général sur la protection des données, la CNIL aidant, de son côté, en dégageant des lignes directrices. Le télétravail en septembre 2021, le droit d'accès en mai 2022, les élections professionnelles en octobre 2022, le recrutement en janvier 2023, le sens des règles est précisé à défaut de disposition propre aux rapports de travail dans le RGPD. Ce dernier, cependant, envisage expressément la possibilité d'élaborer, dans des conventions collectives qui peuvent être des accords d'entreprise, des règles spécifiques dans ce domaine. Le dossier du mois est consacré, dans ce contexte, à apporter des éclairages et des réflexions sur trois thèmes : le recrutement, le droit d'accès des salariés aux données qui les concernent et la place de la négociation collective.

Le recrutement : éclairage sur les principaux points de vigilance pour traiter les données des candidats en toute conformité BJT202r6

Blandine Allix
Avocat au barreau de Paris
Associée, Flichy Grangé Avocats

Justine Février
Avocate au barreau de Paris
Flichy Grangé avocats

Entré en vigueur depuis maintenant cinq ans, le Règlement général sur la protection des données (RGPD) a contraint les entreprises à mettre en place un certain nombre de mesures visant à assurer au quotidien la conformité de l'ensemble de leurs traitements de données à caractère personnel.

Si elles ont été très vite sensibilisées au fait qu'étaient en premier lieu concernées les données de leurs salariés, les entreprises n'ont pas nécessairement réalisé que ce règlement européen – qui reprend la plupart des grandes règles qui étaient déjà prévues par la loi *Informatique et Libertés* (L. n°

78-17, 6 janv. 1978) – s'applique également aux données qu'elles sont amenées à collecter des candidats lors d'une procédure de recrutement. Or, la donnée étant, selon l'article 4, 1), du RGPD, « toute information se rapportant à une personne physique identifiée ou identifiable », les entreprises collectent nécessairement, directement ou indirectement, de nombreuses données à caractère personnel de leurs candidats : nom, prénom, date et lieu de naissance, diplômes, précédentes expériences professionnelles, etc.

Depuis quelques années, les caractéristiques de ces données ont changé. Tout d'abord, le volume des données. Celui-ci est nettement plus important qu'avant grâce aux réseaux sociaux comme LinkedIn ou plus largement internet qui permet d'obtenir de nombreuses informations sur des personnes. Ensuite, la nature des données. Il arrive fréquemment aujourd'hui qu'aux lieu et place de l'envoi des classiques CV et lettre de motivation, le candidat adresse au recruteur une vidéo dans laquelle il se présente et fait part de ses motivations, amenant alors le recruteur à collecter l'image et la voix du candidat.

En outre, la puissance des technologies grâce à l'intelligence artificielle fait que dorénavant, les recruteurs peuvent, par exemple, « scanner » les émotions des candidats lors d'entretiens de recrutement en visioconférence.

Aussi, et dans la mesure où ses précédentes recommandations en la matière dataient de 2002, la CNIL a publié le 30 janvier 2023, après l'avoir soumis à la consultation du public, un « Guide recrutement – Les fondamentaux en matière de protection des données personnelles et questions-réponses ».

Ce guide de 100 pages, organisé sous forme de 19 fiches pratiques à destination aussi bien des entreprises que des cabinets de recrutement, traite des grands principes applicables en matière de recrutement issus du RGPD et de la loi *Informatique et Libertés*.

Il va même plus loin puisqu'à plusieurs reprises, il aborde des questions réglementées par le Code du travail. La CNIL s'en justifie en précisant, dans son guide, en page 61, que « bien que la CNIL ne soit pas en charge de l'application du droit du travail, elle peut le prendre en compte dans le cadre de l'évaluation de la conformité des traitements de données aux règles de la protection des données. En effet, un traitement qui violerait les dispositions du Code du travail en matière de recrutement ne saurait être considéré comme licite au sens du RGPD ».

Les sanctions (administratives, financières, voire pénales) auxquelles les entreprises, les sociétés d'intérim, les cabinets de recrutement s'exposent en cas de non-conformité, peuvent être lourdes de conséquence. Il est donc impératif de s'assurer que les pratiques internes sont bien conformes.

Voici les principaux points de vigilance à avoir en-tête et à respecter.

Des formalités à accomplir avant même de collecter des données de candidats

Avant même de collecter des données de candidats dans le cadre d'un processus de recrutement, plusieurs formalités préalables sont à accomplir dont certaines sont prévues par le Code du travail.

Les obligations prévues par le Code du travail sont principalement les suivantes. D'une part, le comité social et économique doit être informé, préalablement à leur utilisation, sur les méthodes ou techniques d'aide au recrutement des candidats ainsi que sur toute modification de celles-ci (C. trav., art. L. 2312-38, al. 1). Une information du candidat est, d'autre part, prévue aux articles L. 1221-9 (« Aucune information concernant personnellement un candidat à un emploi ne peut être collectée par un dispositif qui n'a pas été porté préalablement à sa connaissance. ») et L. 1221-8 du Code du travail selon lequel « le candidat à un emploi est expressément informé, préalablement à leur mise en œuvre, des méthodes et techniques d'aide au recrutement utilisées à son égard ».

D'autres sont prévues par le RGPD. Tout d'abord, tous les traitements liés au recrutement doivent être inscrits au registre des activités de traitement (RGPD, art. 30 et 57 et art. 100 de la loi *Informatique et Libertés* « LIL »). Le cas échéant, une analyse d'impact pour la protection des données (AIPD) devra avoir été mise en œuvre en cas de traitement susceptible d'engendrer un risque élevé pour les droits et libertés des candidats. Selon la CNIL, la mise en œuvre préalable pourrait se poser pour des traitements utilisés pour tester des candidats via des jeux de rôle ou de logique. En outre, le responsable de traitement – le futur employeur, le cabinet de recrutement ou les sociétés d'intérim – doit également donner préalablement au candidat un certain nombre d'informations. Doivent ainsi être notamment communiqués la finalité du traitement, les destinataires des informations, leur durée de conservation, le caractère obligatoire ou facultatif de la fourniture de l'information, les droits relatifs à ses données à caractère personnel, les pays dans lesquels seront transférées ces données. L'ensemble de ces informations à donner au candidat est listé dans la fiche 8 du guide du recrutement de la CNIL. Cette information permet aux candidats de connaître la raison précise de la collecte des différentes informations personnelles (par exemple : évaluation

des compétences professionnelles, constitution d'une CV-thèque), de comprendre l'usage qui serait fait de ces informations (qui peut les consulter ?, pourquoi ?, combien de temps ?) et de maîtriser l'utilisation de leurs données en facilitant l'exercice de leurs droits.

Théoriquement, cette information peut être orale ou écrite. Naturellement, dans la mesure où le recruteur doit s'assurer que le candidat a bien reçu l'information, il est fortement conseillé de la faire par écrit. En pratique, cette information peut se faire sur le site internet de l'entreprise dans la rubrique recrutement ou faire l'objet d'une information insérée directement dans l'offre d'emploi. Ces supports permettent de faire une information générale et complète visant, notamment, l'ensemble des sources indirectes (site internet type LinkedIn) pouvant être consultées dans le cadre du recrutement.

Cette information doit être donnée préalablement à la collecte et au plus tard au moment même de la collecte, sauf à ce que le recruteur ait collecté des informations de manière indirecte (sur les réseaux sociaux par exemple). Dans ce cas, le responsable de traitement dispose d'un délai maximal d'un mois après la collecte pour informer le candidat du recueil de ses informations et de leur traitement.

La collecte d'informations strictement nécessaires au recrutement du candidat

Le recruteur doit veiller à collecter des informations concernant le candidat qui sont strictement nécessaires à son éventuel recrutement.

Cette logique est non seulement issue du RGPD mais également du Code du travail. On sait que l'un des grands principes du RGPD est le principe de minimisation des données prévu à l'article 5 qui prévoit notamment qu'elles doivent être « adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées ». Ce principe de minimisation rejoint finalement une règle prévue par l'article L. 1221-6 du Code du travail qui prévoit que « Les informations demandées, sous quelque forme que ce soit, au candidat à un emploi ne peuvent avoir comme finalité que d'apprécier sa capacité à occuper l'emploi proposé ou ses aptitudes professionnelles. Ces informations doivent présenter un lien direct et nécessaire avec l'emploi proposé ou avec l'évaluation des aptitudes professionnelles. » Aussi, les informations demandées doivent uniquement permettre d'identifier le candidat le plus adapté au poste à pourvoir et vérifier les compétences et les qualifications requises.

Il en résulte qu'il est en principe interdit de recueillir des informations (i) qui portent sur la vie privée du candidat et ne relèvent pas du contexte professionnel, (ii) dépourvues de lien direct et nécessaire avec l'emploi proposé ou l'évaluation de ses aptitudes professionnelles (iii) et qui pourraient conduire à une discrimination du candidat. Par conséquent, demander par exemple au candidat son numéro de sécurité sociale lors d'un entretien de recrutement est excessif : ce numéro – révélateur de nombreuses données personnelles comme sa date et son lieu de naissance – n'est pas, au stade de l'entretien de recrutement, une information ayant en principe un lien direct et nécessaire avec l'emploi proposé. Il en est de même d'informations laissant apparaître directement ou indirectement, la prétendue origine raciale ou ethnique, les opinions politiques, philosophiques ou religieuses ou les appartenances syndicales, la santé ou la vie sexuelle du candidat. Cette logique de minimisation est applicable aux justificatifs qu'il est possible de demander aux candidats. Ainsi, un recruteur peut parfaitement demander un certificat de travail pour que le candidat justifie avoir réellement occupé les anciens postes dont il se prévaut dans le cadre de ses expériences professionnelles. En revanche, demander un bulletin de paie est disproportionné.

Ce principe de minimisation est relativement aisé à respecter lorsque les recruteurs sollicitent les informations du candidat. Il l'est moins lorsqu'il reçoit spontanément du candidat des informations non sollicitées. Ainsi par exemple d'une candidature spontanée d'un candidat qui joint son CV faisant apparaître, par exemple, ses activités bénévoles dans la paroisse de son quartier. Se pose alors la question de la position que le recruteur doit adopter. La CNIL répond à cette problématique dans son guide. Elle explique, de manière pragmatique, que ces données peuvent être conservées le temps du recrutement, sans que l'entreprise ait besoin de les « masquer », mais qu'en revanche, elles ne peuvent être extraites et utilisées par le recruteur ni déterminer un recrutement.

Une vigilance absolue dans l'utilisation des nouveaux outils technologiques au service du recrutement

La CNIL distingue deux types d'outils technologiques au service du recrutement : d'une part, les outils technologiques permettant la captation de vidéo, de son et parfois leur enregistrement, leur transmission, voire l'analyse par un algorithme des expressions captées du candidat ; d'autre part, les logiciels de tri, de classement et d'évaluation des candidatures.

S'agissant des simples outils permettant de faire passer aux candidats des entretiens en visioconférence sans qu'ils aient à se déplacer, ce qui est un avantage considérable lorsque le candidat est à l'étranger, la CNIL attire l'attention, dans son guide, sur le fait que certaines de ces technologies ne sont pas toujours sécurisées. Elle indique que des outils procéderaient parfois à la collecte de données sans aucun lien avec le processus de recrutement (ex : copie des contacts enregistrés dans le carnet d'adresses du téléphone portable du candidat). D'autres intégreraient des « pisteurs publicitaires » qui permettent de collecter à l'insu du candidat sa géolocalisation, la liste de ses applications ou les comptes associés au terminal. Certains iraient même jusqu'à compromettre la sécurité du matériel informatique du candidat.

Face à ces nouvelles technologies et aux risques qu'elles présentent, la CNIL insiste sur la démarche à suivre pour choisir le bon outil et donne trois principaux conseils qui devront être suivis *a minima* par le responsable IT en vérifiant un certain nombre d'informations auprès du fournisseur sur la fiabilité de son outil et sa conformité au RGPD : le fonctionnement est-il transparent à l'égard des personnes concernées ? Le principe de minimisation des données à caractère personnel collectées est-il respecté tout comme la vie privée du candidat (possibilité de flouter l'arrière-plan, etc.) ? Y a-t-il un transfert de données vers des pays tiers et dans l'affirmative, est-il encadré juridiquement ? La CNIL recommande que cette réflexion soit formalisée par écrit et fasse le cas échéant l'objet d'une analyse d'impact relative à la protection des données (AIPD).

S'agissant plus particulièrement des outils capables de procéder à une analyse par un algorithme des expressions captées du candidat, la démarche devra être identique mais la CNIL indique très clairement qu'« en l'état actuel de la recherche, la fiabilité des résultats obtenus à partir des micro-expressions faciales ne semble pas avoir été corroborée par des études scientifiques sérieuses. Partant, l'utilisation de cet outil dans le cadre de recrutement devrait être écartée ». Par conséquent, un recruteur utilisant ce type d'outil technologique devra être capable de démontrer la fiabilité scientifique de l'outil en cas de contrôle. Il ne pourra pas se contenter d'indiquer que le candidat a donné son accord pour être évalué avec ce type d'outil.

S'agissant enfin des logiciels de tris, leur objet est d'aider les recruteurs dans la prise de décision sur la base de critères prédéterminés et de classement. Leur utilisation aboutit dans certains cas à une prise de décision par la machine sans aucune intervention humaine. Le logiciel peut, en effet, écarter un certain nombre de candidatures afin que le recruteur n'en examine qu'un nombre réduit. Il s'agit donc, concernant les candidatures qui n'auront pas été examinées par le recruteur car automatiquement écartées par le logiciel, d'une décision prise à leur égard de manière « entièrement automatisée ». Il est intéressant de noter que l'appréciation par la CNIL du caractère entièrement automatisé du traitement est très large. Il ne s'agit pas seulement du cas du logiciel qui remettrait au recruteur uniquement les trois meilleures candidatures en écartant les autres. Il peut également s'agir, selon la CNIL, du logiciel qui trie les candidatures et dont on suppose que le recruteur ne regardera que les premières candidatures compte tenu du nombre important de candidatures reçues, non pas celles figurant à la fin du classement, de sorte qu'elles auront ainsi fait l'objet d'une décision entièrement automatisée. La CNIL précise que dans le cas d'une décision entièrement automatisée prise à son égard, le candidat a le droit de demander un second examen humain de sa candidature : le « Human in the Loop » prévu à l'article 22 du RGPD qui pose le principe d'un droit de ne pas faire l'objet d'un traitement entièrement automatisé. Pour que ce droit soit effectif, la CNIL considère que le recruteur devra non seulement informer préalablement le candidat de l'utilisation de ce type de logiciel mais également lui faire part de deux dates importantes qui devront précéder l'étape de finalisation du recrutement : la date à laquelle le candidat devra considérer que sa candidature a été rejetée sur la base d'une décision exclusivement automatisée et la date jusqu'à laquelle il pourra exercer son droit d'obtenir une intervention humaine.

L'utilité de la documentation de la réflexion menée dans le choix du traitement : « *comply to explain* »

Dans plusieurs fiches pratiques, le guide de la CNIL précise qu'il convient, pour le responsable de traitement, de « documenter » sa réflexion (v. ci-dessus s'agissant des logiciels de tri). Cette recommandation va plus loin que le simple registre d'activité de traitement qu'il convient de tenir régulièrement à jour. L'objectif est d'être en mesure de démontrer principalement les démarches entreprises par le recruteur pour s'assurer de la fiabilité et de la conformité de son outil de recrutement au RGPD, les raisons qui l'ont amené à utiliser tel traitement plutôt qu'un autre, sa pertinence, sa proportionnalité au regard de la finalité poursuivie. La documentation constitue donc plutôt une « bonne pratique » permettant aux responsables de traitement de se mettre en conformité avec les règles relatives au RGPD et au droit du travail et de le démontrer en cas de contrôle. Aussi, une absence de documentation de la réflexion ne sera pas en soi

sanctionnée par la CNIL qui s'attachera à sanctionner les manquements au RGPD (comme par exemple le manque de base légale). Mais l'existence de cette documentation sera très utile en cas de contrôle, surtout si cette réflexion avait été menée à l'époque par une personne qui a depuis quitté l'entreprise.

L'épineuse question de la durée de conservation des données des candidats

Les responsables de traitement s'interrogent régulièrement sur la durée de conservation des données à appliquer en l'absence de réponse, que ce soit dans le Code du travail (sauf rares exceptions) ou dans le RGPD.

Pour la durée de conservation des données à caractère personnel, la CNIL propose depuis plusieurs années différentes étapes : la « base active » pour les données auxquelles le responsable de traitement doit avoir accès régulièrement, dans un « environnement immédiat » comme le définit la CNIL, pour la bonne exécution d'un contrat par exemple ; la « base intermédiaire » lorsque la consultation des données peut se révéler indispensable mais de manière ponctuelle et par un nombre limité de personnes (notamment par le service juridique en cas de contentieux) ; enfin l'« archivage définitif » qui permet selon la CNIL d'archiver des données sans limitation de durée dans des conditions très strictes. Comme le précise la CNIL, les délais de prescription des actions contentieuses peuvent constituer un critère permettant d'ajuster la durée de conservation des données.

S'agissant des données de candidats, la CNIL suit la même méthode en distinguant la situation des candidats non retenus de celle des candidats recrutés.

La CNIL recommande pour les candidats non retenus de conserver les données à caractère personnel dans une base active jusqu'à trois mois après l'aboutissement du processus de recrutement afin de pouvoir leur expliquer les raisons de cette décision. Si le candidat y consent, il est possible de conserver ses données après la prise de décision pour une durée plus longue fixée suivant le type de poste dans la limite de deux ans maximum à compter du dernier contact (la CNIL précise que cette durée de conservation doit avoir pour seul objectif de recontacter le candidat en cas de nouvelles opportunités ou d'alimenter une base de données de type « vivier de candidats »). La CNIL précise qu'à l'expiration de cette durée de deux ans, cette opération pourra être renouvelée, donc toujours avec le consentement du candidat. Concernant la base intermédiaire, la CNIL précise que les données à caractère personnel des candidats peuvent être conservées cinq ans à compter de la date de décision d'embauche afin de conserver les preuves nécessaires pour se défendre en cas d'action en discrimination par exemple. On comprend donc que si la durée de deux ans précitée a été renouvelée à nouveau pour deux ans, la durée en base intermédiaire ne pourra être que d'un an en théorie. Cette durée devrait toutefois pouvoir être plus longue si le responsable de traitement peut le justifier (action judiciaire engagée par le candidat toujours en cours par exemple).

La CNIL recommande pour les candidats retenus de conserver les données le temps de la procédure de recrutement jusqu'à la décision d'embauche. À l'issue de cette décision, les données strictement nécessaires pourront être conservées en base intermédiaire à des fins probatoires. Celles utilisées et conservées à des fins de gestion du personnel pourront faire l'objet d'un nouveau traitement avec une nouvelle finalité qui ne sera plus la gestion du recrutement mais la gestion du personnel.

La CNIL fait également un focus sur les agences d'intérim. Elle précise que dans le cas spécifique des viviers de candidats constitués par des agences d'intérim, les données du candidat peuvent être maintenues en base active y compris après la décision de placement du candidat au sein de l'entreprise utilisatrice. À l'expiration de son contrat de mission ou de placement, le candidat pourra ainsi se voir proposer des offres par l'agence d'intérim. Elle précise que le candidat est libre de demander le retrait de son dossier à tout moment.

Ainsi, la durée de conservation doit être déterminée en fonction des besoins. L'objectif est de ne conserver la donnée que si elle est utile et pendant le temps strictement nécessaire. La CNIL précise d'ailleurs en conclusion que « ces durées de conservation ne constituent qu'un point de repère dont le recruteur est libre de s'éloigner sous réserve de documenter son choix et de le justifier ».

Focus sur le droit d'accès des candidats à leurs données à caractère personnel

Comme toute personne dont les données font l'objet d'un traitement, le candidat bénéficie des droits qui lui sont conférés à ce titre par la loi *Informatique et Libertés* et le RGPD, lesquels comportent néanmoins certaines limites. Il s'agit, notamment, du droit d'accès à ses données, du droit de rectification, du droit à l'effacement, du droit d'opposition, du droit de limitation.

Aujourd'hui, le droit exercé majoritairement est le droit d'accès. Même si les demandes de droit d'accès

sont plus généralement formulées par les salariés, il n'est pas exclu qu'un candidat exerce ce droit. Il permet au candidat d'obtenir auprès du responsable de traitement la confirmation que ce dernier possède ou non des données le concernant, certaines informations relatives aux caractéristiques du traitement (finalités poursuivies, durées de conservation projetées, destinataires, etc.) et surtout la copie de ses données. Le recruteur dispose alors d'un délai d'un mois à compter de la réception de la demande pour communiquer ses données au candidat, délai qui peut être prolongé de deux mois (en prenant soin d'en informer le candidat par écrit) en cas de demande complexe ou importante (par exemple lorsqu'un candidat demande l'intégralité de ses données).

Si le recruteur est dans l'impossibilité de communiquer ces données (par exemple si ces données ont été effacées), il doit en informer le candidat dans un délai d'un mois maximum, expliquer les motifs de son inaction et l'informer de la possibilité d'introduire une réclamation auprès de la CNIL et de former un recours juridictionnel.

Comme le précise le RGPD, le droit d'accès n'est pas illimité. D'une part, il ne s'applique qu'aux données de la personne concernée. Par conséquent, le candidat ne peut avoir accès aux données des autres candidats et le recruteur doit veiller, lorsqu'il communique à un candidat une copie d'un extrait d'un document auquel il a droit dans le cadre du droit d'accès, à masquer les éventuelles données des tiers. D'autre part, la communication de ces données ne devra pas porter atteinte aux droits des tiers : principalement secret des affaires, propriété intellectuelle, droit à la vie privée, secret des correspondances. On soulignera qu'une correspondance a été définie par les tribunaux comme « toute relation par écrit existant entre deux personnes identifiables, qu'il s'agisse de lettres, de messages ou de plis fermés ou ouverts.

« Cette relation est protégée par la loi, dès lors que le contenu qu'elle véhicule est exclusivement destiné par une personne dénommée à une autre personne également individualisée, à la différence des messages mis à disposition du public » (v. TGI Paris, 2 nov. 2000, n° 9725223011, confirmé par CA Paris, 17 déc. 2001, n° 00-07565). En vertu de cette définition, des échanges internes d'e-mails entre le DRH et le manageur intéressé pour recruter le candidat, dans lesquels le DRH et ledit manageur évoqueraient la candidature de l'intéressé, devraient être qualifiés de correspondances protégées par le secret et ne pas être communiqués au candidat exerçant son droit d'accès.

Conclusion

Face à ces nombreuses obligations, les recruteurs ont tout intérêt à prendre en main ce guide illustré de nombreux exemples pragmatiques destiné à les accompagner au cours des différentes étapes du recrutement. À toutes fins utiles, il est précisé que pour les TPE-PME, la CNIL a également élaboré une synthèse de questions-réponses incontournables en matière de recrutement.

Enfin, pour tester leur conformité au RGPD, les recruteurs peuvent s'auto-évaluer en remplissant le questionnaire d'auto-évaluation en cinq étapes proposé par la CNIL. Ce questionnaire leur permettra de vérifier étape par étape si les principes clés et les exigences imposées par la réglementation sont respectés.

Demande de droit d'accès par les salariés à leurs données personnelles : faut-il tout communiquer ? BJT202s5

Julie Schwartz
Avocate au barreau de Paris
Hogan Lovells

Joséphine Beaufour
Avocate au barreau de Paris
Hogan Lovells

Les demandes de droit d'accès exercées par les salariés auprès de leurs employeurs ou anciens employeurs sont de plus en plus fréquentes, et y répondre peut s'avérer être un exercice délicat, voire périlleux, pour l'employeur.

Au titre de l'article 15 du Règlement Général sur la Protection des Données, le « RGPD » (Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, règlement général sur la protection des données), un salarié, au même titre que toute autre personne physique, est légitime à exercer son droit d'accès pour connaître les données personnelles le concernant traitées par son employeur, afin notamment d'identifier comment et à quelles fins celles-ci sont traitées. Ces demandes doivent donc être prises au sérieux, en y apportant une réponse la plus précise possible.

L'exercice est d'autant plus difficile car, dans la pratique, le droit d'accès consacré à l'article 15 du RGPD tend à être détourné de sa finalité première. Il est en effet majoritairement exercé par des salariés ayant fait l'objet d'une sanction disciplinaire, ou en cours de procédure de licenciement, ou parfois même en phase de recrutement par une entreprise concurrente. Dans ces situations, le droit d'accès peut devenir un véritable instrument de collecte d'informations auxquelles le salarié n'aurait pas pu avoir accès ou n'a plus accès (par exemple, ses emails professionnels), ou bien aurait dû pour y accéder recourir à d'autres procédés (par exemple, une requête au titre de l'article 145 du Code de procédure civile dans le cadre d'une procédure contentieuse), lui permettant notamment de collecter des preuves en vue d'un contentieux prud'homal, ou de partager à son futur employeur des informations clés sur des pratiques ou décisions stratégiques de l'entreprise.

L'exercice du droit d'accès s'avère également être un outil efficace dans un contexte de précontentieux ou contentieux pour un salarié et/ou son conseil qui analyseront précisément toutes les données personnelles qui auront été communiquées par l'(ex)employeur en réponse à la demande de droit d'accès, afin d'y déceler des points de non-conformité à la réglementation applicable (par exemple, des données qui ont été communiquées par l'entreprise en réponse à la demande de droit d'accès et qui n'auraient pas dû être conservées par l'entreprise), et de dénoncer ensuite ces manquements à la Commission nationale de l'informatique et des libertés (la « CNIL »). L'exercice est d'autant plus ardu lors de demandes émanant de salariés présents depuis de très nombreuses années dans l'entreprise et pour lesquelles un grand nombre de données personnelles a été et est encore traité par l'employeur, ce qui peut nécessiter de mobiliser de façon importante des ressources au sein de l'entreprise pour répondre à la demande.

Or, la CNIL est très vigilante sur la question du respect, par l'employeur, du droit d'accès exercé par les salariés, et se contente rarement d'un simple rappel à l'ordre lorsqu'une plainte à ce sujet lui est adressée. L'autorité n'hésite pas à solliciter de la part de l'employeur davantage d'informations sur la manière dont les données personnelles des salariés sont traitées, et l'invite bien souvent à se justifier sur les manquements allégués. En cas de réponse insatisfaisante, une procédure d'instruction, pouvant aboutir à une sanction, peut être ouverte.

Face à l'accroissement des demandes de droit d'accès, comment préserver les intérêts de l'entreprise tout en répondant, conformément à la réglementation

applicable, aux demandes exercées par les salariés ? Comment satisfaire à ces demandes sans engager des coûts et moyens humains et financiers disproportionnés ? Comment faire le tri dans toutes les données personnelles du salarié traitées par l'entreprise ? Et surtout, est-il obligatoire de tout communiquer pour répondre à de telles demandes ?

Voici ci-après quelques clés, accompagnées de nombreux exemples, qui nous semblent pouvoir être utiles à mobiliser dans le cadre de l'élaboration d'une réponse à une demande de droit d'accès.

I. Qu'est-ce que le droit d'accès ?

A. Présentation du droit d'accès

Le droit d'accès est la possibilité pour une personne physique, par exemple un salarié d'une entreprise, de demander à un responsable du traitement, par exemple son employeur ou ancien employeur, à accéder à ses données personnelles traitées et conservées par ce dernier, sous format papier ou sous forme électronique dans ses systèmes d'information.

Ce droit découle des droits fondamentaux à la protection de la vie privée et à la protection des données à caractère personnel, respectivement consacrés aux articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne. C'est la raison pour laquelle il est difficile de limiter ce droit : toute dérogation faite par un employeur, décidant de ne pas communiquer certaines données en réponse à une demande de droit d'accès, doit en effet s'opérer dans les limites du strict nécessaire (CJUE, 11 déc. 2014, n° C-212/13, *Ryneš* : « La protection du droit fondamental à la vie privée, garanti par l'article 7 de la charte, exige que les dérogations à la protection des données à caractère personnel et les limitations de celle-ci s'opèrent dans les limites du strict nécessaire »).

B. Modalités pratiques pour répondre à une demande de droit d'accès

Les modalités applicables à l'exercice des droits des personnes concernées sont exposées à l'article 12 du RGPD, et celles spécifiques au droit d'accès à l'article 15 du RGPD. Par ailleurs, pour aider le responsable du traitement à répondre à une demande de droit d'accès, le Comité Européen de la Protection des Données (« CEPD ») a publié des lignes directrices (« Guidelines 01/2022 on data subject rights – Right of Access », Lignes directrices du CEPD n° 01/2022 adoptées le 18 janvier 2022), et la CNIL quelques recommandations (« Le droit d'accès des salariés à leurs données et aux courriels professionnels », CNIL, 5 janv. 2022), consultables sur leurs sites internet respectifs.

Pour satisfaire à une demande de droit d'accès, l'employeur dispose d'un délai initial d'un mois à compter de la réception de la demande pour fournir au salarié une copie des données à caractère personnel le concernant. Ce délai peut toutefois être prolongé de deux mois supplémentaires, compte tenu de la complexité et du nombre de demandes d'accès auxquelles l'employeur doit répondre.

Il est donc primordial pour l'employeur, dans un premier temps, d'accuser réception de la demande du salarié en lui indiquant le délai de réponse, et en motivant, le cas échéant, une éventuelle prolongation de ce délai.

Si le salarié présente sa demande sous forme électronique, l'employeur devra, si possible, lui fournir une copie de ses données personnelles par voie électronique également, à moins que le salarié ne demande qu'il en soit autrement. À titre d'exemple, si le volume des données personnelles à communiquer est important, celles-ci pourront être communiquées au salarié via une « data room » dont les identifiants pour s'y connecter pourront lui être adressés par email.

C. Les limites du droit d'accès

Le droit d'accès, au titre de l'article 15 du RGPD, ne concerne que l'accès aux données personnelles de la personne en faisant la demande, et non l'accès aux documents contenant ces données personnelles. La façon dont le droit d'accès est actuellement détourné implique que les demandes exercées portent bien souvent sur des copies de documents.

Or, l'article 15 du RGPD se limite à permettre l'accès à des données personnelles et aux informations sur la façon dont ces données sont traitées, et n'offre en aucun cas un accès automatique aux documents les contenant. La CNIL rappelle d'ailleurs que « Le droit d'accès porte uniquement sur les données personnelles et non pas sur des documents » et que c'est uniquement si cela est « plus pratique » pour l'employeur qu'il peut décider de communiquer des documents mais que cela « n'est pas obligatoire » (« Le droit d'accès des salariés à leurs données et aux courriels professionnels », CNIL, 5 janv. 2022).

Si les données personnelles sont communiquées via une « data room » par exemple, celle-ci ne doit contenir que la copie des données personnelles, et non la copie de l'intégralité des documents contenant ces données personnelles. Ainsi, l'employeur peut, et est légalement autorisé à, se limiter à :

– fournir uniquement une liste des données personnelles qu'il traite concernant le salarié (par exemple, nom, prénom, matricule, date de naissance, poste dans l'entreprise, etc.) ; ou

– fournir les documents contenant les données personnelles du salarié en masquant, manuellement ou de manière automatisée, toutes les informations contenues dans les documents qui ne sont pas les données personnelles du salarié.

L'option du partage de fichiers caviardés est, dans la plupart des cas, privilégiée pour permettre au salarié de pouvoir comprendre dans quel contexte ses données sont traitées.

II. Les pièges à éviter

Afin de préserver les intérêts de l'entreprise, il est essentiel, avant toute réponse à une demande de droit d'accès, de :

– (i) bien identifier le périmètre de la demande du salarié, et éventuellement de lui demander de repréciser sa demande si celle-ci est excessive par exemple ;
– (ii) vérifier que les données personnelles et documents qui seront éventuellement communiqués sont légitimes à être conservés par l'entreprise et peuvent donc être communiqués ; et
– (iii) s'assurer que les informations pouvant porter atteinte aux droits des tiers ont bien été masquées.

A. Les demandes excessives ou infondées du salarié

Comme nous l'indiquions précédemment, l'employeur dispose d'un délai serré pour répondre aux demandes de droit d'accès qu'il reçoit, qui peuvent par ailleurs requérir une charge de travail conséquente. Une demande excessive peut ainsi être parfois difficile à satisfaire dans le délai imparti par le RGPD.

L'article 12.5 du RGPD émet une première réserve à la satisfaction d'une demande d'accès « lorsque les demandes d'une personne concernée sont manifestement infondées ou excessives, notamment en raison de leur caractère répétitif ». Dans cette hypothèse, l'employeur, en tant que responsable du traitement, peut :

– exiger le paiement de frais raisonnables qui tiennent compte des coûts administratifs supportés pour fournir les informations, procéder aux communications ou prendre les mesures demandées ; ou
– refuser de donner suite à ces demandes.

La notion de demande « infondée » doit s'entendre de manière restrictive (v. section 6.3.1 des Lignes Directrices du CEPD n° 01/2022 : « Therefore, the EDPB emphasises that there is only very limited scope for relying on the "manifestly unfounded" alternative of Art. 12(5) GDPR in terms of requests for the right of access »). Ainsi, il est admis qu'une demande d'accès manifestement infondée soit caractérisée uniquement si elle ne remplit pas les conditions de l'article 15.3 du RGPD à savoir que les données sollicitées (i) ne constituent pas des données personnelles, (ii) ne font pas l'objet d'un traitement par le responsable du traitement ou (iii) ne concernent pas la personne physique exerçant la demande.

Quant à la notion de demande « excessive », l'article 12.5 du RGPD indique simplement que cette condition est caractérisée *notamment* en raison de son caractère répétitif, sans pour autant dresser une liste exhaustive des motifs ou seuils caractérisant la répétition.

En pratique, il peut être considéré par exemple qu'un employeur pourrait refuser de faire droit à une nouvelle demande de droit d'accès d'un salarié qui fait suite à trois demandes exercées au cours des trois mois précédents. Une demande manifestement excessive pourrait également être caractérisée lorsque cette demande nécessite la mise en œuvre de moyens disproportionnés de la part de l'employeur. L'exemple type est celui d'un salarié employé depuis plusieurs années au sein de l'entreprise et demandant, sans autre précision, à avoir accès à l'intégralité de ses données personnelles collectées et traitées par l'employeur depuis son recrutement.

À titre d'exemple, le Sénat avait estimé lors des débats sur le projet de modification de la Loi Informatique et Libertés (L. n° 78-17, 6 janv. 1978 relative à l'informatique, aux fichiers et aux libertés) qu'était « manifestement abusive » (ce terme ayant été par la suite remplacé par « excessive ») une demande « particulièrement étendue, parce qu'elle portait par exemple sur une durée de quinze ans » (Rapp. Sénat n° 218, 19 mars 2003, p. 126). L'autorité belge de protection des données personnelles (l'« APD ») a quant à elle considéré, dans une décision du 9 février 2021, qu'un employeur était fondé à refuser une demande de droit d'accès dans la mesure où (i) la demande d'accès portait sur des données personnelles collectées depuis l'entrée en fonction en 2008 de l'auteur de la demande, jusqu'à la cessation de son contrat de travail en 2019 (soit sur une période de plus de 10 ans), et (ii) l'ex-salarié auteur de la demande n'apportait aucune explication quant à l'intérêt de sa demande, « la Chambre Contentieuse ne [pouvant] dès lors percevoir de besoin spécifique justifiant la charge de travail importante que représenterait la fouille systématique liée à la demande d'accès à l'ensemble des logs IT le concernant » (APD, Chambre Contentieuse, décision n° 15/2021, 9 févr. 2021).

Dans une autre affaire plus récente du 3 avril 2023 (APD, Chambre Contentieuse, décision n° 40/2023, 3 avr. 2023), l'APD a retenu la même appréciation à propos de la requête d'un salarié visant à obtenir accès à l'ensemble de ses emails, sans autre critère plus précis de recherche, en motivant sa décision notamment par

ces termes : « la Chambre Contentieuse constate que la recherche de tous les e-mails concernant [l'auteur de la demande d'accès] sur une durée d'au moins 8 ans, après la fin de l'occupation, représenterait une charge de travail disproportionnée pour [l'employeur] ».

Comme indiqué précédemment, le droit d'accès découlant du droit fondamental de la protection des données à caractère personnel, toute dérogation à celui-ci doit se faire dans la stricte limite du nécessaire. L'employeur devra donc être précautionneux en utilisant le motif de demande excessive ou infondée comme motif de refus. En effet, le refus de l'employeur opposé au salarié au simple motif d'une demande excessive par exemple pourrait être facilement contesté. Une attention particulière doit donc être portée par l'employeur lorsqu'il utilise ce motif, ce qui implique notamment de :

– justifier auprès du salarié les raisons pour lesquelles la demande est considérée comme manifestement excessive (par exemple, au regard de son ancienneté, du nombre de documents sollicités, du caractère répétitif de sa demande, etc.) ; et
– ne pas fermer la porte en opposant un refus définitif mais inviter plutôt le salarié à repréciser sa demande (par exemple, en visant des échanges d'emails sur une période précise ou avec des interlocuteurs spécifiques ou bien portant sur un sujet en particulier, en ne sollicitant que certaines catégories de documents comme les fiches de paie ou les comptes-rendus d'évaluation professionnelle, etc.).

Si le salarié refuse de préciser sa demande, ou ne répond pas à l'invitation à la repréciser par exemple, le refus au motif de demande manifestement excessive opposé par l'employeur aura plus de force et sera plus difficilement contestable.

B. Les durées de conservation applicables aux données personnelles et documents sollicités dans le cadre de la demande de droit d'accès

Le traitement d'une demande de droit d'accès est souvent l'occasion pour un employeur de revoir sa politique de durée de conservation en matière de ressources humaines.

Dans la plupart des cas, les données personnelles du salarié traitées par l'employeur peuvent être conservées pendant toute la durée du contrat de travail du salarié en base active, puis en archivage pour les durées de prescription légale applicables.

Toutefois, quelques exceptions sont à connaître.

Par exemple, la CNIL recommande que les logs de badges d'accès des salariés aux locaux de l'entreprise, conservées à des fins de contrôle individuel de l'accès pour sécuriser l'entrée dans les bâtiments, soient supprimés 90 jours après leur collecte (« L'accès aux locaux et le contrôle des horaires sur le lieu de travail », CNIL, 5 mai 2019). Les données des badges utilisées pour le suivi du temps de travail doivent quant à elles être conservées au maximum 5 ans à compter de leur collecte.

Les images étant considérées comme des données personnelles au sens du RGPD, celles issues des caméras de vidéosurveillance peuvent également faire l'objet d'une demande de droit d'accès au titre de l'article 15 du RGPD. Ces images ne peuvent toutefois être conservées plus d'un mois après leur captation (« La vidéosurveillance – vidéoprotection au travail », CNIL, 23 juill. 2018).

Les enregistrements de conversations téléphoniques mises en place, par exemple, à des fins d'évaluation professionnelle, de formation des salariés ou encore d'amélioration du service, et auxquelles participe un salarié dans le cadre de ses fonctions, doivent être supprimés au bout de six mois après leur collecte (Norme simplifiée n° 57 (27 nov. 2014) de la CNIL et recommandations de la CNIL sur l'écoute et l'enregistrement des appels sur le lieu de travail, 5 mai 2019).

D'autres durées de conservation spécifiques s'appliquent également. L'employeur doit donc être très vigilant, avant de répondre à une demande d'accès, à ce qu'il puisse justifier que les données qu'il s'apprête à communiquer puissent être encore présentes légalement dans ses systèmes d'information.

Ces précautions s'appliquent également aux documents, le cas échéant, que décide de communiquer l'employeur dans le cadre d'une réponse à une demande de droit d'accès. Recrutement, gestion de la paie, formation professionnelle, gestion des congés et des absences, déclarations sociales, élections professionnelles, surveillance des locaux, etc., sont en effet autant de finalités poursuivies par un employeur qui impliquent un nombre conséquent de données personnelles traitées.

Dans certains cas, ces données peuvent être contenues dans des copies de documents fournies par le salarié lui-même, par exemple lors de son recrutement ou au cours de sa carrière, puis stockées dans les systèmes d'information de l'entreprise.

La première question que l'employeur doit se poser avant de communiquer de tels documents à l'auteur de la demande d'accès est : suis-je légitime à conserver une copie de ces documents ? En effet, deux des principes cardinaux du RGPD sont la légitimité de la finalité de traitement (RGPD, art. 5.1, b) et la minimisation des données (RGPD, art. 5.1, c). L'employeur peut ainsi tout à fait être légitime à demander à un salarié de lui fournir des copies de certains documents,

mais n'est pas nécessairement conforme aux principes de légitimité et minimisation s'il les conserve.

Par exemple, lorsqu'un salarié se marie ou se pacse, ce dernier peut bénéficier d'un congé rémunéré de quelques jours. Afin de s'assurer que le salarié est éligible à ce congé, l'employeur lui demande une copie de son certificat de mariage ou de PACS. En revanche, une fois cette information vérifiée, l'employeur n'apparaît plus légitime à conserver la copie du certificat puisque l'information a pu être vérifiée et la finalité du traitement est donc réalisée. En outre, ce document comprend de nombreuses données personnelles, notamment celles relatives au conjoint du salarié, dont l'employeur ne pourrait justifier leur collecte et traitement au titre du principe de minimisation. La conservation de la simple information « certificat de mariage ou de PACS vérifié : Oui/Non » apparaît donc amplement suffisante pour répondre aux principes de légitimité de la finalité du traitement et de minimisation des données personnelles collectées et traitées. La copie du document transmise peut ensuite être détruite par l'employeur. Lors d'une demande de droit d'accès, ledit document n'ayant pas été conservé, celui-ci ne fera pas l'objet d'une communication par l'employeur au salarié et le salarié ne pourra ainsi contester la légitimité de la conservation dudit document par l'employeur.

Il en est de même pour le permis de conduire dont l'original ne pourra être conservé par l'employeur que si cela est strictement nécessaire. Par exemple, si la copie du permis avait été collectée par l'employeur au moment de l'attribution d'un véhicule de fonction au salarié, mais que ce dernier n'en bénéficie désormais plus, l'employeur n'a aucune raison de conserver ce document dans ses systèmes d'information.

En communiquant, dans le cadre d'une réponse à un droit d'accès, les copies de documents conservés illicitement dans ses systèmes d'information, l'employeur s'expose au risque que le salarié adresse une plainte aux services de la CNIL.

III. Les secrets opposables

L'article 15.4 du RGPD apporte une limite supplémentaire au droit d'accès, disposant que « le droit d'obtenir une copie [des données à caractère personnel] visée au paragraphe 3 ne porte pas atteinte aux droits et libertés d'autrui ».

Le considérant (63) du RGPD précise la portée de cet article en indiquant que « ce droit ne devrait pas porter atteinte aux droits ou libertés d'autrui, y compris au secret des affaires ou à la propriété intellectuelle, notamment au droit d'auteur protégeant le logiciel ».

Cette liste n'est pas exhaustive, le législateur européen ayant pris le soin de préciser dans le considérant (63) « y compris », pouvant par conséquent être complétée par d'autres principes issus du droit de l'Union ou le droit d'un État membre.

A. Le secret des affaires

En exerçant une demande de droit d'accès, un salarié peut solliciter un accès à ses données personnelles qui seraient contenues dans des documents faisant état par ailleurs d'un secret des affaires de l'entreprise, tel que défini à l'article L. 151-1 du Code de commerce.

En pratique, cette situation se produit généralement lorsque l'auteur de la demande dispose d'un poste dont les fonctions nécessitent qu'il ait accès à des informations sensibles, confidentielles ou stratégiques de l'entreprise. C'est d'ailleurs ce qu'a relevé l'APD dans sa décision du 9 février 2021 (APD, Chambre Contentieuse, décision n° 15/2021, 9 févr. 2021) précédemment évoquée qui admet que :

– « en raison de sa fonction de cadre, [l'auteur de la demande d'accès] a connaissance de l'identité des clients de [l'employeur], des montants des commandes et des factures à ces clients, qui constituent des informations potentiellement sensibles sur les affaires de [l'employeur] » ; et
– « [l'auteur de la demande d'accès] demande la copie de l'intégralité des emails dans lesquels il est destinataire ou expéditeur ».

L'autorité belge en a conclu que l'employeur « n'a pas violé l'article 15.1 et 3 [du RGPD] en refusant de donner suite à la demande de [l'auteur de la demande d'accès] de copie des emails dans lesquels il est destinataire ou expéditeur », et ce au regard « des informations potentiellement sensibles contenues dans les emails en question ».

Toutefois, il peut être en pratique très difficile de démontrer une atteinte au secret des affaires :

– d'une part, parce que le secret des affaires tend à limiter le droit fondamental à la protection des données, et doit donc être interprété de façon restrictive ; et
– d'autre part, parce que seules les informations revêtant une valeur économique peuvent être protégées au titre du secret des affaires, ce qui n'est pas le cas de toutes les informations contenues dans les fichiers et emails qui peuvent être sollicités par le salarié.

Le secret des affaires peut donc être utilisé comme fondement pour restreindre le champ des informations communiquées dans le cadre d'une réponse à une demande de droit d'accès, mais doit être particulièrement bien justifié et circonscrit.

B. Le secret professionnel

L'obligation de confidentialité qui pèse sur un salarié disposant d'informations confidentielles dans le cadre de l'exercice de ses fonctions professionnelles est le corollaire du lien de subordination et de l'exécution du contrat de travail. Ce secret, consacré par l'article 226-13 du Code pénal, permet à un employeur d'imposer à son salarié une obligation de confidentialité à l'égard des tiers, mais également d'interdire à ce dernier de détourner de sa finalité une information qui lui est accessible à l'occasion de l'exécution de ses missions professionnelles.

Dans la mesure où un salarié peut librement disposer d'une information qui lui serait transmise au titre de son droit d'accès, ce dernier serait en mesure de la transmettre à quiconque ou de la diffuser publiquement. Il peut donc exister un conflit direct entre l'obligation de confidentialité d'un salarié et la transmission, dans le cadre d'une demande de droit d'accès, d'un document contenant ses données personnelles et qui révèle par exemple une activité de l'entreprise réalisée à travers les missions du salarié.

Le règlement de ce conflit impose à l'employeur de ne fournir au salarié au titre du droit d'accès que des informations qui ne sont pas susceptibles de révéler une activité professionnelle de l'entreprise ou une information confidentielle.

Ainsi, si la demande de droit d'accès implique de communiquer un document qui pourrait contenir à la fois des informations couvertes par le secret professionnel et des données personnelles d'un salarié, il est nécessaire que le caviardage effectué sur le document permette une décontextualisation complète du document, de telle sorte qu'il ne puisse plus révéler aucune information confidentielle et ne conserve que les données personnelles sollicitées.

C. Le secret des correspondances

Le salarié peut, au titre de l'article 15 du RGPD, également solliciter l'accès à ses données personnelles figurant dans les emails contenus dans sa boîte électronique, voire même dans certains cas, dans des emails dont il n'est ni l'expéditeur, ni le destinataire.

Or, ces emails peuvent également contenir des informations relatives à des tiers qui sont protégées par le secret des correspondances, conformément à l'article 226-15 du Code pénal.

Lorsque le salarié est l'expéditeur ou le destinataire des emails, la CNIL estime que « la communication des courriels est présumée respectueuse des droits des tiers » dans la mesure où « le salarié a déjà eu, ou est supposé avoir eu connaissance des informations contenues dans les messages visés par la demande » (« Le droit d'accès des salariés à leurs données et aux courriels professionnels », CNIL, 5 janv. 2022). La CNIL poursuit en indiquant que dans cette situation « l'anonymisation ou la pseudonymisation des données relatives aux tiers constitue une bonne pratique, et non une condition préalable à la transmission des courriels ».

Lorsque le salarié souhaite obtenir la communication de données personnelles contenues dans des emails dans lesquels il est mentionné mais n'est ni l'expéditeur ni le destinataire, la CNIL précise que « l'employeur doit trouver un équilibre entre la satisfaction du droit d'accès du salarié et le respect des droits et libertés des autres salariés, notamment le secret des correspondances ». Pour ce faire, la CNIL indique que l'employeur doit, dans un premier temps, identifier si les emails visés par la demande suppose la mise en œuvre de moyens particulièrement intrusifs tels que le scan de l'ensemble des messageries des salariés de l'entreprise. Ce sera dans la plupart des situations bien évidemment le cas.

Dans cette hypothèse, la CNIL indique que l'employeur doit par conséquent demander à l'auteur de la demande de droit d'accès de préciser sa demande :

– Si le salarié refuse de préciser sa demande d'accès, ou ne précise pas suffisamment ladite demande, l'employeur est légitime de ne pas répondre favorablement à la demande d'accès de son salarié ou ex-salarié.
– Si le salarié précise correctement sa demande, l'employeur doit alors, selon la CNIL, étudier le « contenu des courriels demandés et apprécie[r] la portée de l'atteinte aux droits des tiers que représenterait leur communication, notamment au regard du secret de la correspondance et de la vie privée de l'émetteur et des destinataires ». Cela ne ferme donc pas la porte à un possible refus de l'employeur. Il demeure ainsi possible pour l'employeur de justifier que la demande porte atteinte aux droits des tiers et au secret des correspondances et ne pas faire droit à la demande.

En tout état de cause, s'il est analysé que la demande du salarié ne porte pas atteinte à l'un des secrets évoqués ci-avant et peut donc être satisfaite, l'application de l'exception découlant de l'article 15.4 du RGPD (« Le droit d'obtenir une copie visé au paragraphe 3 ne porte pas atteinte aux droits et libertés d'autrui »), que ce soit pour préserver le secret des affaires, le secret des correspondances ou bien préserver l'obligation de confidentialité, implique pour l'employeur de caviarder les documents avant de pouvoir satisfaire à la demande du salarié.

Il ressort des éléments ci-dessus que l'exercice du droit d'accès par les salariés auprès de leurs employeurs ou anciens employeurs n'emporte pas un droit auto-

matique d'obtenir communication de toute information et de tout document sollicités. La demande doit rentrer dans le champ de l'article 15 du RGPD et l'employeur dispose de nombreux arguments juridiques pour justifier de ne communiquer que certains éléments, tout en étant conforme au RGPD. Il n'est donc pas requis légalement de systématiquement tout communiquer lorsque l'on reçoit une demande de droit d'accès. Une analyse au cas par cas, prenant en compte le contexte de la demande, la relation avec le salarié et le périmètre de sa demande demeure toutefois nécessaire pour chaque demande.

La négociation relative aux données à caractère personnel BJT202s9

Grégoire Loiseau
Professeur à l'école de droit de la Sorbonne (Paris 1)

Alors que l'article 88 du règlement général sur la protection des données envisage expressément la possibilité de concevoir, par des conventions collectives qui peuvent être des accords d'entreprise, des règles spécifiques au traitement dans les relations de travail des données des employés, la timidité du dialogue social en la matière interroge sur l'intérêt réel de la négociation collective. La démarche, pour l'apprécier, emprunte deux parcours, l'un pour sonder l'utilité pratique de la négociation, l'autre pour réfléchir au contenu celle-ci.

1. Les traitements de données à caractère personnel peuvent-ils faire l'objet de règles particulières issues de la négociation collective ? Au-delà de la règlementation en vigueur, y a-t-il une place, autrement dit, pour des aménagements conventionnels ? L'interrogation est sérieuse en présence d'un appareil normatif pétri d'impérativité. Sans doute, l'ordre public, à moins d'être absolu, n'empêche pas la conclusion d'accords collectifs dont le contenu présente un caractère plus favorable. Le règlement général sur la protection des données personnelles (RGPD) donne, qui plus est, une visibilité à part entière aux conventions collectives. L'article 88 en fait le moyen de prévoir, dans les relations de travail, des règles spécifiques au traitement des données des employés. Alors que le règlement européen ne comporte pas lui-même de disposition propre aux relations de travail, il permet aux États membres de procéder, dans ce domaine, à des spécifications, soit par la loi, soit au moyen de conventions collectives qui peuvent être « des accords d'entreprise »[1]. Ces règles d'appoint, sensibilisées au milieu professionnel, peuvent concerner « notamment », d'après le texte, des traitements opérés aux fins de recrutement, d'exécution ou de résiliation du contrat, de gestion et d'organisation du travail, de protection de la santé et de la sécurité au travail, etc.

Dans les faits, il ne semble pas pourtant que les partenaires sociaux se soient emparés de ce sujet de négociation pour élaborer des règles qui ajoutent à la règlementation en vigueur. À l'occasion d'un atelier organisé en mars 2022 par la CNIL avec des syndicats, ces derniers ont évoqué, comme une piste d'action, la possibilité de faire de la protection des données personnelles un sujet collectif et d'activer l'article 88 du RGPD. Mais ils ont suggéré que la CNIL commence par inciter d'y recourir dans ses supports relatifs à la protection des données personnelles au travail, ce qui « contribuerait certainement à orienter la vision des acteurs vers la voie du dialogue collectif »[2]. Quant à la pratique conventionnelle, son examen fait ressortir la conclusion de nombreux accords comportant des stipulations relatives aux données à caractère personnel et à la protection qui leur est accordée, majoritairement lorsqu'ils ont pour objet l'organisation du vote électronique. Dans une moindre mesure, certains accords en traitent à propos de l'utilisation des

1 Règlement européen, cons. 155.

2 Atelier CNIL, Syndicats et représentants des travailleurs, sept. 2022, p. 6.

outils numériques[3], du télétravail ou de l'exercice du droit syndical. Mais, dans l'ensemble, ces accords se bornent à rappeler les règles applicables – notamment en termes d'information ou de droits des salariés[4] – à préciser les mesures de sécurité à prendre[5], parfois à signaler les catégories de données traitées, par exemple à l'occasion de l'usage des outils numériques[6].

2. Cette timidité du dialogue social n'est pas à mettre sur le compte des syndicats ou sur celui des employeurs mais, plus probablement, sur une retenue *a priori* à appréhender les problématiques liées aux traitements de données personnelles en marge de la règlementation en vigueur. Se mêlent à cet égard le sens de l'impérativité des règles, qui laissent peu de place à des normes d'appoint, et la difficulté de maîtriser leur niveau d'exigence et leur portée de manière suffisamment sûre pour se projeter au-delà de leur stricte observation. La sollicitation de la CNIL pour qu'elle incite, dans les documents qu'elle publie, à conclure des accords collectifs éclaire parfaitement la préoccupation d'être assuré de ce qui peut être fait en matière de négociation collective. La circonstance que le RGPD soit un texte général qui ne consacre pas de disposition propre aux relations de travail n'aide pas, de fait, les partenaires sociaux à conceptualiser des aménagements conventionnels spécifiques à l'entreprise. Et, de son côté, le droit du travail ne propose pas d'occasions franches de s'intéresser aux questions de protection des données à caractère personnel. La négociation obligatoire sur la qualité de vie au travail étendue, depuis la loi du 2 août 2021, à la qualité des conditions de travail peut, il est vrai, prêter à des échanges à ce sujet. Mais il n'est pas flagrant, pour le moment, que les accords conclus en matière de qualité de vie et des conditions de travail (QVCT) révèlent un intérêt pour ces problématiques.

La question se repose, dans ces conditions, de savoir s'il existe un intérêt qui ne serait pas simplement théorique à faire du traitement de données à caractère personnel et des modalités de leur protection un objet de négociation. La démarche pour l'apprécier peut emprunter deux parcours, l'un pour s'interroger sur l'utilité de la négociation collective, l'autre pour réfléchir au contenu de celle-ci.

I. L'utilité de la négociation collective

3. L'utilité de la négociation répercute l'intérêt d'un accord qui devrait conjuguer, ici, l'intérêt des salariés et celui de l'employeur. Un accord au seul profit du collectif des salariés est en effet peu vraisemblable en la matière alors que le niveau de protection assuré par la règlementation applicable est élevé et que les contraintes incompressibles qui pèsent sur l'employeur sont fortes. S'il n'est donc pas exclu que des mesures plus favorables que celles prévues par le RGPD soient adoptées, il est plus probable que les normes négociées prévoient, selon les termes de l'article 88 du règlement, « des règles plus spécifiques » au cadre des relations de travail. C'est d'ailleurs l'esprit de l'article 88 qui n'est pas tant de rendre possibles des dérogations *in melius* que de permettre la conception de règles, d'ordre législatif ou de nature conventionnelle, prenant en compte l'environnement professionnel dans lequel des traitements de données personnelles sont nécessairement opérés. Intitulé « Traitement de données dans le cadre des relations de travail », le texte affiche cet objectif et témoigne incidemment de la conscience que la collecte et l'utilisation de données dans les rapports de travail peut justifier « des règles plus spécifiques ». Le législateur français n'a pas pris cette option, à la différence, notamment, de la législation fédérale allemande[7]. Mais cela ne préjuge pas de l'opportunité d'y procéder au moyen d'accords collectifs de travail.

La norme conventionnelle pourrait d'ailleurs, dans cet objectif, être plus pertinente que la loi car elle présente l'avantage de posséder un degré de précision et de proximité avec les préoccupations concrètes des entreprises qui font défaut à la norme légale. Ces qualités, particulièrement recherchées aujourd'hui – ce que manifeste la faveur pour l'accord d'entreprise –, servent la norme conventionnelle lorsqu'il en est attendu de donner une dimension opérationnelle aux principes de protection des données personnelles en intégrant les particularités d'un secteur d'activité spécifique et/ou les particularités des activités de traitement. Des règles spécifiques peuvent, par exemple, être utiles quand l'entreprise traite des données sensibles, qui peuvent être celles des salariés – comme des données biométriques – ou celles de ses clients – comme des données de santé. L'accord collectif peut avoir pour objet de déterminer les garanties perti-

3 V. novateur, Accord mondial sur les droits des salariés du groupe Société Générale, 28 juin 2023, article 5.1 relatif à la numérisation et aux droits numériques.

4 Par ex. Accord sur l'aménagement du temps de travail, SCP de chirurgiens Noël-Thomson-Brenougat-Pentoux, 25 juin 2021.

5 Par ex. Charte utilisateur informatique et moyens de télécommunication, Dynacité, 8 juill. 2021.

6 Par ex. Avenant modifiant l'accord relatif à l'exercice du droit syndical, Banque de France, 26 oct. 2022.

7 La loi fédérale sur la protection des données (*Bundesdatenschutzgesetz, BDSG*), entrée en vigueur le 25 mai 2018, comporte des dispositions sur le traitement des données personnelles des salariés (§ 26 BDSG) et sur l'obligation de désigner un délégué à la protection des données et sur sa protection (§ 38 BDSG). Les premières comprennent, notamment, des règles spécifiques sur les conditions d'efficacité du consentement du salarié.

nentes à appliquer aux données collectées auprès de tiers ou des mesures de sécurité spécifiques, les modalités de communication ou de diffusion des données sous l'angle, notamment, de leur degré de confidentialité, des échéances de conservation adaptées, les mécanismes de gestion des données au titre de l'exercice des droits des personnes, etc.

4. L'utilité de la négociation collective est aussi celle de la norme conventionnelle par rapport à d'autres types de normes pouvant avoir le même objet. Dans les espaces accessibles à des « règles plus spécifiques » en sens de l'article 88 du RGPD, une large part d'entre elles peuvent être adoptées unilatéralement par l'employeur. Elles peuvent être établies en fonction des situations et des besoins de l'entreprise ou rendues plus pérennes dans un document qui les formalisent. On pense alors à une charte, puisque le modèle est à la mode, dont le contenu peut être diversement mis à profit pour exposer la politique de l'entreprise en matière de protection des données personnelles, sensibiliser les salariés aux problématiques des traitements qui les concernent ou/et qui concernent les clients, les informer de leurs droits et déterminer les mesures qu'ils doivent eux-mêmes, le cas échéant, respecter. On conviendra que ce type de charte n'est pas encore vraiment développé. Des entreprises ont bien adopté des chartes de protection ou d'utilisation des données personnelles, mais à destination de leurs clients[8]. À l'attention des salariés, c'est plutôt pour le moment dans le cadre d'autres chartes – le plus souvent des chartes informatiques ou relatives aux outils numériques – que des dispositions sont consacrées aux traitements et à la protection des données à caractère personnel.

Charte ou accord collectif ? Le choix dépend de plusieurs facteurs à prendre en considération. La force normative des mesures spécifiques, s'il y en a, est un premier facteur. Alors que la charte se prête mieux à un contenu comprenant des éléments d'information et/ou des normes régulatoires – sous la forme de lignes directrices, de recommandations, etc. –, l'accord collectif a par nature un contenu prescriptif. La différence n'est pas toutefois irréductible, la charte pouvant avoir une autorité renforcée si elle est annexée au règlement intérieur tandis qu'un accord collectif peut parfaitement comporter des contenus informatifs ou/et relevant du droit souple[9]. Un deuxième facteur est l'évolutivité des contenus qu'il est plus facile de modifier dans une norme unilatérale qu'au sein d'un accord collectif. Il faut également tenir compte, c'est un troisième facteur, du rayonnement de chaque type de norme. De ce point de vue, les indices de confiance et de sécurité juridique sont certainement plus élevés en présence d'une norme négociée adoptée dans le cadre d'un accord collectif que lorsque l'employeur en est unilatéralement l'auteur. Cela peut aider, le cas échéant, à établir le respect du RGPD même si l'application de la norme ne peut garantir, en soi, la conformité aux prescriptions du règlement. Il y a enfin certains sujets dont il ne peut être traité que par accord collectif et pour lesquels une norme unilatérale serait ineffective. Spécialement, la détermination dans des contextes spécifiques de l'intérêt légitime, au sens de l'article 6 du RGPD qui en fait l'une des bases juridiques du traitement, ne serait pas opposable opérée unilatéralement par l'employeur alors qu'elle constitue un enjeu de négociation collective.

5. Un autre type de normes pouvant concurrencer les accords collectifs sur les questions donnant prise à la négociation collective rassemble celles élaborées dans le cadre de codes de conduite. Prévus à l'article 40 du RGPD, ces codes partagent une préoccupation en partie commune avec celle des accords collectifs puisqu'ils sont destinés, d'après le texte, à contribuer à une bonne application du règlement compte tenu de la spécificité des différents secteurs de traitement ou/et des besoins spécifiques des micro, petites et moyennes entreprises. Ils ont pour objet de fixer des règles concernant, entre autres choses, la transparence des traitements, l'intérêt légitime du responsable de traitement considéré dans des contextes spécifiques, l'information des personnes concernées, l'exercice de leurs droits, etc. Confiés à l'initiative d'organisations représentatives d'un secteur d'activité, comme des fédérations professionnelles, ils sont juridiquement contraignants et obligent les adhérents à se conformer aux règles qu'ils énoncent. Encore doivent-ils, pour cela, être approuvés par la CNIL, enregistrés et publiés.

Les risques de chevauchement sont cependant, pour l'heure, inexistants, aucun code approuvé par la CNIL n'ayant été publié depuis l'entrée en vigueur du RGPD. Les instruments ne s'inscrivent pas, de toute façon, dans la même perspective. Les codes de conduite sont conçus dans une démarche sectorielle pour faciliter au moyen de règles concrètes précises le respect de l'exigence de conformité par les responsables de traitement et pour harmoniser les pratiques dans les secteurs concernés. Ils s'adressent en cela aux entreprises du secteur d'activité et s'imposent à celles d'entre elles qui sont adhérentes de l'organisation qui en a pris l'initiative tandis que, vis-à-vis des salariés qui ne sont pas forcément seuls concernés, ils contribuent à améliorer leur protection. Les accords collectifs sont

8 Par ex. Charte de protection des données personnelles d'EDF ; Charte des données personnelles du groupe Crédit Agricole.

9 Pensons aux accords relatifs aux modalités d'exercice du droit à la déconnexion.

pour leur part négociés et conclus dans une démarche de proximité avec la situation de l'entreprise – même si des accords de branche ne sont pas à exclure – et rendent applicables, aussi bien à l'employeur qu'aux salariés, des règles plus spécifiques que celles du RGPD afin de faire face à des problématiques propres aux relations de travail. Le contenu de la négociation collective permet de s'en rendre compte.

II. Le contenu de la négociation collective

6. Si l'exercice est vain d'improviser le contenu des accords collectifs sans l'expérience de la pratique, encore très pauvre, on peut, à la lumière des textes, en esquisser certains contours et se faire une idée des questions ouvertes à la négociation. L'article 88 du RGPD lui-même signale différents aspects des relations de travail donnant lieu à des traitements de données qui pourraient faire l'objet de « règles plus spécifiques » par voie législative ou conventionnelle. Le texte évoque le recrutement, l'exécution du contrat, la gestion, la planification et l'organisation du travail, l'égalité et la diversité sur le lieu de travail, la santé et la sécurité au travail, la protection des biens appartenant à l'employeur ou au client, l'exercice et la jouissance des droits et des avantages liés à l'emploi, individuellement ou collectivement, ou encore la résiliation de la relation de travail.

Sans prétendre à l'exhaustivité – l'article 88 emploie d'ailleurs l'adverbe « notamment » –, on peut ajouter à ces questions le contrôle exercé au moyen de technologies numériques[10], l'évaluation des salariés[11] ou, dans le champ du collectif, l'exercice des droits syndicaux et en particulier la communication syndicale lorsqu'elle emprunte les canaux de l'entreprise (intranet, messageries professionnelles), sans oublier évidemment les élections organisées par voie électronique. L'utilisation des outils numériques et, le cas échéant, de systèmes d'intelligence artificielle constitue du reste une autre orientation pour envisager des sujets de négociation dans la mesure où elle induit la collecte et l'usage de données personnelles dans des conditions qui ne sont pas encore, pour certaines, encadrées par le droit positif. C'est un champ accessible aux accords collectifs pour normer des pratiques en développement.

7. En affinant l'analyse, il y a tout de même des éléments de contenu de la négociation plus assurés que d'autres. Avec l'idée que la valeur ajoutée de l'accord collectif soit de sécuriser certains traitements de données, plusieurs sujets de négociation peuvent être identifiés. Le premier sujet est directement suggéré par l'article 9 du RGPD qui, posant un principe d'interdiction des traitements portant sur des données sensibles – données génétiques, données biométriques, données de santé, etc. –, assortit le principe d'exceptions dont l'une d'elles est la nécessité du traitement pour l'exécution d'obligations ou l'exercice de droits propres au responsable du traitement ou à la personne concernée en matière de droit du travail, de sécurité sociale et de protection sociale. Le texte précise que l'exception suppose que le traitement soit autorisé par le droit d'un État membre ou par une convention collective prévoyant des garanties appropriées pour les droits fondamentaux et les intérêts des personnes concernées. Concrètement, l'employeur pourrait donc être autorisé à collecter certaines données sensibles pour l'exécution de ses obligations ou l'exercice de ses droits propres si un accord collectif le prévoit. La CNIL l'a d'ailleurs expressément envisagé en matière de recrutement, considérant qu'une convention collective pourrait autoriser la collecte de données sensibles s'agissant d'une entreprise de tendance à condition que la convention intègre des garanties appropriées pour les droits fondamentaux et les intérêts des candidats concernés[12].

Un autre sujet de négociation est la détermination de l'intérêt légitime de l'employeur de procéder à un traitement particulier lorsqu'il ne dispose pas d'une autre base juridique pour le justifier, spécialement celle tirée de la nécessité du traitement pour l'exécution des contrats de travail. Le règlement européen y voit une question pouvant donner lieu à des précisions dans le cadre de codes de conduite[13], ce qui devrait faire admettre, *mutatis mutandis*, d'en traiter également dans le cadre d'un accord collectif. L'identification d'un intérêt légitime fondant la mise en œuvre d'un traitement, lorsqu'elle est opérée par voie conventionnelle, est un moyen de sécuriser l'application de cette base juridique dans des contextes spécifiques, même s'il n'en résulte pas une garantie de conformité du traitement avec la règlementation sur la protection des données personnelles.

Dans le même ordre d'idée, qui est de sécuriser des traitements par des règles spécifiques qui comprennent, en tant que de besoin, des mesures appropriées pour protéger les intérêts légitimes des salariés, un accord collectif peut programmer ces règles pour fixer un cadre normatif au transfert de données au sein d'un groupe de sociétés. L'article 88 du RGPD, à l'alinéa 2,

10 L'article 88 du RGPD mentionne à l'alinéa 2 les « systèmes de contrôle sur le lieu de travail » parmi les traitements auxquels il y a lieu d'accorder « une attention particulière ».

11 Les appréciations et avis concernant une personne sont considérés, de manière générale, constituer des données à caractère personnel : CJUE, 4 mai 2023, n° C-487/21, F.F. c/ Österreichische Datenschutzbehörde ; JCP G 2023, 914, doctr. G. Loiseau.

12 CNIL, Guide du recrutement, 30 janv. 2023, spéc. p. 99.

13 L'article 40 du RGPD vise à ce sujet « les intérêts légitimes poursuivis par les responsables du traitement dans des contextes spécifiques ».

mentionne ce type d'opération parmi celles auxquelles il y a lieu d'accorder « une attention particulière »[14]. Le considérant 48 du règlement indique à ce sujet que les responsables de traitement qui font partie d'un groupe d'entreprises « peuvent avoir un intérêt légitime à transmettre des données à caractère personnel au sein du groupe à des fins administratives internes, y compris le traitement de données à caractère personnel relatives à des clients ou des employés ». Chaque entreprise du groupe ayant alors la qualité de responsable de traitement dans un tel type d'opération réalisée, par exemple, pour des besoins de gestion RH, un cadre normatif est utile afin d'organiser ces flux dans le respect des droits des salariés. Un accord collectif, qui serait ici un accord de groupe, peut en être l'instrument profitant des atouts de la norme négociée en termes de confiance et de sécurité juridique.

Ces qualités sont aussi recherchées par des accords collectifs qui auraient pour objet de conventionnaliser des bonnes pratiques. Ces pratiques ont pu être expérimentées au sein de l'entreprise elle-même. Les partenaires sociaux peuvent également s'inspirer des recommandations et lignes directrices de la CNIL. L'autorité administrative en a publié plusieurs dans le domaine des relations de travail, à propos du télétravail à l'époque où ce mode d'organisation de l'activité était recommandé dans le contexte de la pandémie de la Covid-19[15], sur le droit d'accès dont disposent les salariés pour obtenir communication des données personnelles traitées par l'employeur[16], sur les problématiques de protection des données à caractère personnel dans l'organisation et le déroulement des élections professionnelles[17] ou encore, plus récemment, en matière de recrutement[18]. Une grande partie de ces orientations ou recommandations peuvent être, il est vrai, appliquées sans qu'il soit besoin de les formaliser dans un accord collectif. Mais il peut être dans l'intérêt des salariés comme dans celui de l'employeur de donner à certaines d'entre elles une force normative contraignante – ce dont elles sont dépourvues en tant qu'elles constituent du droit souple – ainsi qu'une visibilité au sein de l'entreprise que n'ont pas les documents publiés par la CNIL. Par exemple, il pourrait être énoncé dans un accord collectif relatif, de manière générale, au traitement de données personnelles ou portant, plus particulièrement, sur le télétravail que l'employeur s'interdit toute surveillance constante au moyen de dispositifs vidéo ou audio mais qu'il peut en revanche être demandé aux salariés d'activer leur caméra pendant une réunion en visioconférence, le cas échéant en recourant à un dispositif de floutage de l'arrière-plan.

8. Un autre volet de la négociation pourrait porter, avantageusement, sur les droits reconnus par le RGPD. Des règles spécifiques auraient du sens pour certains de ces droits afin d'aménager leur exercice dans un triple objectif : favoriser la transparence quant aux données traitées[19], garantir l'effectivité des droits par des mesures simples de mise en œuvre – ce qui peut incidemment favoriser la confiance – et éviter au moyen d'un cadre normatif que des droits soient improprement exercés. On pense bien sûr d'abord, à ce sujet, au droit d'accès dont le rôle est essentiel pour assurer l'exercice d'autres droits – droit de rectification, droit à l'effacement – mais qui est prétexte aujourd'hui à des demandes sans rapport avec sa finalité[20]. Ces demandes sont, au vrai, le plus souvent le fait d'anciens salariés qui ne seraient pas concernés par l'accord collectif. Un tel accord n'en serait pas moins utile pour mettre à la disposition des salariés une procédure interne d'accès aux données considérées, pour déterminer le ou les supports de communication des données en question et pour garantir leur intelligibilité en les rendant accessibles de façon compréhensive tout en signalant clairement que la transmission d'une copie n'implique pas celle du document qui les contient[21].

Des règles spécifiques seraient également profitables pour normer l'exercice du droit à la portabilité qui peut être mobilisé des salariés souhaitant que des données ayant fait l'objet d'un traitement automatisé au cours de l'exécution de leur contrat leur soient fournies dans un format structuré, couramment utilisé, afin de les transmettre à un autre responsable de traitement[22], par exemple un nouvel employeur. Outre la mise en place d'une procédure interne pour répondre aux demandes dans les délais[23], il peut s'agir d'organiser, lorsque c'est techniquement possible, la transmission directe des données d'un responsable de traitement à l'autre ou de prévoir la mise au point par l'employeur de formats interopérables pour permettre la portabi-

14 L'article 88 vise le « transfert de données à caractère personnel au sein d'un groupe d'entreprises, ou d'un groupe d'entreprises engagées dans une activité économique conjointe ».

15 CNIL, Questions-réponses du 8 septembre 2021 sur le télétravail.

16 CNIL, « Le droit d'accès des salariés à leurs données et aux courriels professionnels », 18 mai 2022.

17 CNIL, Questions-réponses du 24 octobre 2022 sur les élections professionnelles.

18 CNIL, Guide du recrutement, 30 janv. 2023 ; JCP S 2023, 56, étude G. Loiseau.

19 L'article 88, alinéa 2, invite à accorder une attention particulière « à la transparence du traitement ».

20 G. Loiseau, « Les débordements du droit d'accès aux données à caractère personnel », JCP S 2022, 1259.

21 Il ne s'agit ici que de rappeler la position de la Cour de justice de l'Union européenne qui juge que « le terme « copie » ne se rapporte pas à un document en tant que tel, mais aux données à caractère personnel qu'il contient et qui doivent être complètes » (CJUE, 4 mai 2023, n° C-487/21, pt 32).

22 RGPD, art. 20.

23 Le délai est en principe d'un mois, porté à trois mois maximum si la demande est complexe (RGPD, art. 12.3).

lité. Plus prosaïquement, l'intérêt de la norme peut être de déterminer les données que l'employeur a recueillies dans le cadre du contrat de travail, distinguées de celles qu'il a recueillies dans le cadre d'une obligation légale, seules les premières faisant l'objet du droit à la portabilité. En pratique, la distinction peut être relativement complexe. Par exemple, un compte rendu d'entretien de suivi de la charge de travail d'un salarié au forfait jours est effectué pour respecter des obligations légales que l'employeur se doit d'appliquer en vertu du contrat de travail. La norme conventionnelle permettrait de fournir des règles sûres.

Enfin, mais sans épuiser la liste des possibles, c'est au droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé auquel les partenaires sociaux pourraient s'intéresser à l'avenir avec le développement des outils de recrutement, de gestion du travail ou d'évaluation algorithmiques. L'intérêt serait notamment de prévoir les modalités d'une intervention humaine, *ex-ante* ou *ex-post*, ou de déterminer les applications nécessaires à la conclusion ou à l'exécution du contrat ou, à défaut, celles qui nécessitent le consentement explicite de la personne dans la mesure où ces applications dérogent à l'interdiction d'une décision entièrement automatisée[24].

La négociation collective a donc bien, tout compte fait, de la matière pour être conduite et pour produire des règles spécifiques à la relation de travail, dont l'apport est réel. Les partenaires sociaux ont un intérêt commun à apporter plus de visibilité, plus de sécurité, plus de précision dans la mise en œuvre de la règlementation. L'appréhender au moyen de normes conventionnelles est certainement le meilleur moyen de se l'approprier.

24 RGPD, art. 22.