N° 375669
Société Renault Trucks

10ème et 9ème sous-sections réunies
Séance du 15 avril 2015
Lecture du 11 mai 2015

CONCLUSIONS

Mme Emilie BOKDAM-TOGNETTI, rapporteur public

Jusqu'où une entreprise peut-elle aller dans la surveillance des connexions internet de ses salariés pour prévenir et détecter la consultation par ceux-ci de fichiers à caractère pédopornographique ? Telle est la question posée, sous l'angle du respect de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, par la présente requête.

Le groupe Volvo, auquel appartient la société Renault Trucks, a, dans le cadre de sa politique d'entreprise dite de « responsabilité sociale et sociétale », décidé de renforcer ses actions de lutte contre la diffusion d'images ou de vidéos à caractère pédopornographique, en déployant sur les ordinateurs des salariés de ses différentes entités un logiciel informatique. Ce logiciel, dénommé « NetClean Pro Active », permet de détecter sur les postes informatiques de l'entreprise la présence de fichiers susceptibles de comporter des images ou vidéos présentant un caractère pédopornographique.

Il fonctionne selon le schéma suivant : un logiciel installé sur chaque poste informatique de l'entreprise scanne et analyse en temps réel les empreintes numériques (ou méta-données) correspondant aux fichiers stockés ou transitant sur ce poste pour les comparer avec une base de données appartenant à l'éditeur du logiciel, établie par ce dernier à partir des empreintes numériques des fichiers déclarés par Interpol comme étant de nature pédopornographique. Cette base est téléchargée et stockée localement sur chaque poste individuel, puis mise à jour régulièrement à distance par le serveur NetClean. En cas d'identification de fichiers communs entre la base et les empreintes des fichiers consultés, stockés ou téléchargés sur le poste, une alerte informatique se déclenche à l'attention de la hiérarchie du groupe, permettant le cas échéant, avec le concours de la police, d'établir le caractère pédopornographique des fichiers et d'identifier leur utilisateur.

La société Renault Trucks a, le 15 novembre 2012, saisi la CNIL d'une demande d'autorisation de mise en œuvre de ce traitement, qu'elle a formalisée par une demande en ligne le 28 novembre 2012. Après demandes de compléments et instruction du dossier, la CNIL a, par une délibération n° 2013-377 du 5 décembre 2013, notifiée par un courrier du 19 décembre 2013, refusé l'autorisation sollicitée. Elle a estimé que le traitement envisagé portait sur des données à caractère personnel relatives à des infractions et en a déduit que, la société n'entrant dans aucune des exceptions prévues par l'article 9 de la loi du 6 janvier 1978 et n'étant par ailleurs pas privée, en cas de refus d'autorisation, de son droit d'exercer un recours

juridictionnel s'agissant des infractions dont elle serait victime, le traitement ne pouvait être autorisé. C'est ce refus dont la société Renault Trucks vous demande l'annulation.

A l'appui de sa requête, la société soulève d'abord trois moyens touchant à la régularité externe de la délibération.

Il est en premier lieu soutenu que la délibération serait irrégulière à défaut de mentionner la date de la demande d'autorisation et, ainsi, de mettre en mesure de vérifier le respect du délai de deux mois prévu par l'article 25, III de la loi du 6 janvier 1978.

Toutefois, aucune disposition n'impose à la CNIL de faire figurer sur ses délibérations une telle mention. Par ailleurs, on ne pouvait avoir de doute, en l'espèce, sur la demande dont il s'agissait, de sorte qu'il ne résulte pas de ce défaut de mention une imprécision qui empêcherait de comprendre la portée de la délibération.

La société fait valoir, en deuxième lieu, que la délibération est irrégulière en ce qu'elle ne mentionne pas ses modalités d'adoption et la majorité obtenue à l'occasion du vote des membres, ne permettant pas de vérifier la conformité de la procédure de vote suivie.

Toutefois, là encore, aucune disposition n'impose de faire figurer de telles mentions. Au demeurant, le procès-verbal produit par la CNIL – qui nous paraît présenter un caractère probant contrairement à ce que soutient la requérante – montre que la commission s'est réunie en séance plénière et que l'absence de deux membres ne l'empêchait pas d'atteindre la majorité absolue de 9 membres.

La dernière critique adressée à la régularité de la délibération est tirée de ce que celle-ci n'a été notifiée avec accusé de réception que le 19 décembre 2013, en violation des dispositions de l'article 15 du décret n° 2005-1309 du 20 octobre 2005 prévoyant que la notification intervient dans un délai de 8 jours après l'adoption de la délibération.

Mais il résulte de votre jurisprudence que les conditions de notification d'une décision sont sans effet sur sa légalité (v. par exemple, pour l'absence d'incidence, sur la légalité d'un refus d'autorisation d'exploitation de fréquences hertziennes, du dépassement du délai prévu pour sa notification par l'article 32 de la loi n° 86-1067 du 30 septembre 1986 : CE, Section, 18 novembre 2011, *Société Quinto Avenio*, n° 321410, au Recueil). Dès lors, pour regrettable que ce soit ce retard, il n'a pas entaché d'illégalité la délibération contestée.

Les moyens d'illégalité externe étant écartés, nous pouvons donc en venir à ceux – plus intéressants – touchant à la légalité interne de la délibération attaquée.

Le premier moyen est tiré de ce que c'est à tort que la CNIL a considéré que des traitements de données à caractère personnel étaient opérés au moyen du système NetClean, alors que seules des données techniques, exclusives de tout caractère personnel, sont collectées puis traitées par ce logiciel.

La société fait valoir, d'une part, qu'au stade de la détection, les empreintes numériques collectées ne sont que des séquences inintelligibles de caractères alphanumériques dont la valeur est produite par un algorithme de hachage, et d'autre part, qu'au stade de la phase d'alerte, toutes les données d'identification de l'utilisateur

(notamment son nom et son prénom) et les données de l'alerte sont chiffrées, selon un processus réversible, et que personne à l'exception des administrateurs habilités au sein du groupe et, le cas échéant, de la police, ne peut voir, lire ou accéder à ces données.

Cette argumentation ne saurait vous retenir. Car si toute donnée informatique se réduit techniquement, par définition, à une suite de chiffres et, parfois, de lettres, la question est de savoir s'il s'agit d'une donnée devenue définitivement inintelligible ou qui peut être décryptée.

En effet, l'article 2 de la loi du 6 janvier 1978 dispose que « *constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne* ».

Or en l'espèce, les responsables sécurité et ressources humaines de la société et les administrateurs de l'interface NetClean disposent des moyens pour, en cas de remontée d'une alerte, déchiffrer les données relatives à l'alerte, lesquelles comportent les nom, prénoms et matricule de l'utilisateur du poste informatique, la localisation de son poste, ses données de connexion ainsi que le nom et le chemin du fichier détecté. Certes, il n'est pas certain, tant qu'une vérification approfondie n'a pas été faite, que l'utilisateur attitré du poste soit bien celui qui a téléchargé les fichiers pédopornographiques, mais ce point nous paraît indifférent à la caractérisation d'une donnée personnelle, qui suppose seulement l'existence d'informations relatives à une personne physique identifiée ou identifiable, et non que ces informations soient nécessairement fiables et exemptes d'erreur.

Le deuxième moyen est tiré de ce que la CNIL ne pouvait considérer que le traitement envisagé permettait de détecter et de collecter des données relatives à des infractions pénales ni appliquer en conséquence l'article 9 de la loi du 6 janvier 1978, alors que le traitement vise uniquement la collecte d'empreintes numériques ne préjugeant pas du contenu effectif du fichier mais révélant uniquement une présomption d'identité avec un fichier contenu dans la base de données NetClean, et que seules les vérifications par les autorités de police permettront d'établir le caractère pédopornographique du fichier et de qualifier l'infraction.

Sur ce point également, l'argumentation de la société ne nous paraît pas devoir prospérer.

L'article 9 de la loi du 6 janvier 1978 prévoit que les traitements de données à caractère personnel relatives aux infractions, condamnations et mesures de sûreté ne peuvent être mis en œuvre que par les juridictions, les autorités publiques et les personnes morales gérant un service public agissant dans le cadre de leurs attributions légales, les auxiliaires de justice pour les stricts besoins de l'exercice des missions qui leur sont confiées par la loi, et les sociétés de perception et de répartition des droits d'auteur.

Contrairement à ce que soutient la société, il nous semble qu'il n'est pas nécessaire qu'un procès-verbal d'infraction ait été dressé par la police et que la justice ait qualifié

pénalement des faits pour qu'une donnée puisse être regardée comme « relative à une infraction » au sens de l'article 9.

D'une part, la loi distingue les données relatives aux infractions et celles relatives aux condamnations. D'autre part, l'article 9 de la loi du 6 janvier 1978 dans sa version issue de la loi du 6 août 2004 comportait initialement un 3° autorisant la mise en place de traitements de données à caractère personnel relatives aux infractions par les personnes morales victimes d'infractions pour les stricts besoins de la prévention et de la lutte contre la fraude ainsi que de la réparation du préjudice. Le Conseil constitutionnel a censuré cette disposition dans sa décision n° 2004-499 DC du 29 juillet 2004, *Loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel*, tout en précisant que l'article 9, tel qu'il résulte de la déclaration d'inconstitutionnalité ainsi prononcée, ne saurait être interprété comme privant d'effectivité le droit d'exercer un recours juridictionnel dont dispose toute personne physique ou morale s'agissant des infractions dont elle a été victime. Il nous paraît résulter de cette réserve que le Conseil constitutionnel a estimé que les données relatives aux infractions ne se limitaient pas aux seules données relatives à des agissements constatés et sanctionnés par les autorités compétentes, car si une donnée relative à une infraction ne pouvait être relative qu'à une infraction déjà qualifiée par le juge, cela suppose que la victime de l'infraction ait déjà été reconnue comme telle par la justice et la réserve relative au droit d'exercer un recours juridictionnel, dont les commentaires aux *Cahiers* indiquent qu'elle était « *indispensable pour ne pas priver de base légale les traitements légitimement mis en œuvre par chaque personne morale pour suivre les dossiers contentieux relatifs aux infractions dont elle a été elle-même victime* », perdrait alors en grande partie de son sens.

Surtout, il nous semble que, pour apprécier si un traitement porte sur des données à caractère personnel relatives aux infractions, il convient de rechercher à quels faits les données se rapportent et de tenir compte de la finalité du traitement et du processus dans lequel il s'inscrit. Or ce traitement, qui transforme l'entreprise en auxiliaire des services de police et de l'autorité judiciaire, a pour finalité explicite la lutte contre la pédopornographie. Même si les faits en cause n'ont pas, lors de la mise en œuvre du traitement, été constatés par la police ni qualifiés au regard de la loi pénale par l'autorité judiciaire, le traitement vise spécifiquement à détecter la consultation et le téléchargement d'images et de vidéos à caractère pédopornographique, c'est-à-dire à détecter des agissements qui, s'ils sont avérés, tombent sous le coup de l'article 227-23 du code pénal, et ne vise à détecter ces faits que parce qu'ils tombent sous le coup de la loi pénale. Le traitement aboutit à informer la police de tels faits, cette information étant expressément prévue dans la procédure d'alerte décrite par l'entreprise si le téléchargement se révèle intentionnel.

Dans ces conditions, il nous semble que le processus NetClean doit être regardé comme mettant en œuvre des traitements de données à caractère personnel relatives à des infractions au sens de l'article 9. Le moyen nous paraît donc devoir être écarté.

Enfin, le dernier moyen est tiré de ce que la demande aurait dû être examinée au regard de l'article 25, I, 4° de la loi du 6 janvier 1978, qui prévoit qu'une autorisation est nécessaire pour la mise en œuvre des « *traitements automatisés susceptibles, du fait de leur nature, de leur portée ou de leurs finalités, d'exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat en l'absence de toute disposition législative ou réglementaire* », et non de l'article 25, I, 3° de cette loi, selon lequel sont mis en œuvre après

autorisation de la CNIL les traitements, automatisés ou non, portant sur des données relatives aux infractions, condamnations ou mesures de sûreté. La société fait valoir que la révélation par les autorités judiciaires, à l'issue du processus NetClean, de l'existence d'un fichier à caractère pédopornographique pourrait avoir pour effet non seulement l'engagement de poursuites judiciaires, mais aussi le déclenchement de mesures disciplinaires susceptibles de priver la personne responsable du bénéfice de son contrat de travail.

Certes, la consultation et le téléchargement d'images pédopornographiques par un salarié sur son poste professionnel constituent une faute grave justifiant son licenciement et, ainsi, la rupture de son contrat (Cass. soc., 15 décembre 2010, *G...*).

Toutefois, eu égard à la finalité du traitement qui est, selon les déclarations de la société elle-même, de lutter dans le cadre de sa politique de responsabilité sociale et sociétale contre la diffusion d'images pédopornographiques, et compte tenu de la réponse apportée au moyen précédent, il nous semble que c'est à bon droit que la CNIL s'est fondée sur le 3° du I de l'article 25 de la loi et non sur le 4° du I du même article.

Les hypothèses concernées par le 4° du I de l'article 25 nous semblent très différentes de celle ici en cause. Il ressort en effet des travaux préparatoires de la loi du 6 août 2004 qu'il s'agit, à titre principal, de viser les traitements de données permettant à des professionnels, par exemple en matière de banque ou d'assurance, de connaître le « profil » de certaines personnes et de décider en toute connaissance de cause de contracter, le cas échéant en fixant des conditions particulières, ou de ne pas contracter.

Vous écarterez donc ce dernier moyen.

Si vous nous suivez, ce que vous jugerez ne désarmera nullement les sociétés, qui disposent déjà de nombreux moyens pour contrôler leurs salariés. En effet, les connexions Internet d'un salarié à partir d'un poste informatique de l'entreprise, de même que les fichiers enregistrés sur son ordinateur professionnel qui ne sont pas indiqués expressément comme personnels, sont présumés présenter un caractère professionnel et l'employeur peut donc les rechercher *a posteriori* pour les identifier et les ouvrir en dehors de la présence du salarié (sur les connexions internet, v. Cass. soc. 9 juillet 2008, *M. L...*, Bull. 2008, V, n° 150 ; Cass. soc. 9 février 2010, *M. M...*; sur les fichiers créés par le salarié : Cass. soc. 10 mai 2012, *Société NCT*, Bull. 2012, V, n° 135). Il lui est loisible, par exemple, de consulter un relevé mensuel des sites consultés et des fichiers téléchargés par un salarié sur Internet afin de vérifier l'absence de connexions ou de consultations de sites à des fins personnelles en violation des obligations découlant du contrat de travail et du règlement intérieur de l'entreprise, tels des sites de rencontre, des sites de jeux, ou encore des sites à caractère pornographique (il existe une abondante jurisprudence de la Cour de cassation sur ce point, v. par exemple Cass. soc. 10 mai 2012, *M. R...*; Cass. soc. 23 novembre 2011, *M. P...*), voire pédopornographique, pour en tirer ensuite des conséquences disciplinaires et, s'il y a lieu, mais sans que cela constitue la finalité de la vérification, en avertir les forces de l'ordre.

Enfin, nous terminerons en indiquant que le téléchargement sur chaque poste du contenu de la base de données NetClean, même si celle-ci se compose d'empreintes numériques cryptées, ne nous paraît pas sans soulever des interrogations au regard de la loi pénale, laquelle dans certaines hypothèses punit à l'article 227-23 du code pénal la fixation,

l'enregistrement ou la transmission d'images à caractère pédopornographiques de mineurs de quinze ans même réalisés sans intention de diffuser ces images, ainsi que leur recel.

Par ces motifs, nous concluons au rejet de la requête.