

Délibération n°2010-072 du 18 mars 2010 de la formation restreinte décidant l'interruption d'un traitement mis en œuvre par la Société M.

18 Mars 2010 - Thème(s) : Biométrie

La Commission nationale de l'informatique et des libertés, réunie en formation restreinte, sous la présidence de M. Alex TÜRK ;

Etant aussi présents M. Emmanuel de GIVRY, vice-président délégué, Mme Isabelle FALQUE-PIERROTIN, vice-présidente, Mme Claire DAVAL, M. Sébastien HUYGHE et M. Jean-Marie COTTERET, membres ;

Vu la Convention n° 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004 ;

Vu le décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifié par le décret n° 2007-451 du 25 mars 2007 ;

Vu la délibération n° 2006-147 du 23 mai 2006 fixant le règlement intérieur de la Commission nationale de l'informatique et des libertés ;

Vu la délibération n° du 25 avril 2007 de la Commission nationale de l'informatique et des libertés refusant la mise en œuvre par la société C. d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès aux locaux ;

Vu le rapport de M. MASSOT, commissaire rapporteur, notifié à la société par huissier le 2 mars 2010 ;

Vu les autres pièces du dossier ;

Après avoir entendu, lors de la réunion du 18 mars 2010 :

M. MASSOT, commissaire, en son rapport ;

Mme ROLIN, commissaire du Gouvernement, en ses observations ;

Madame D. , gérante, et Monsieur O. , responsable administratif et financier de la société M. ,

Madame D. et Monsieur O. ayant pris la parole en dernier.

I. Faits et procédure

A. Faits

La société M. (ci-après « la société ») a pour activité le commerce de gros d'habillement et de chaussures destinés au secteur militaire, sous l'enseigne... La société, qui a changé de dénomination sociale le 13 août 2009, exerçait auparavant ses activités sous la dénomination C.

La délibération de la CNIL du 25 avril 2007 refusant d'autoriser à la société C. à mettre en œuvre des dispositifs biométriques reposant sur l'empreinte digitale

a société C. a déposé le 19 juillet 2006 une demande d'autorisation auprès de la Commission nationale de l'informatique et des libertés (ci-après, « la CNIL » ou « la Commission »), préalablement à la mise en œuvre d'un dispositif biométrique reposant sur l'empreinte digitale (dossier n° .). La demande visait tant le dispositif d'accès aux bureaux que le dispositif d'accès à la salle informatique contenant les serveurs.

La Commission a examiné ce dossier lors de sa séance plénière du 25 avril 2007 en faisant application des critères régulièrement établis pour se prononcer sur les demandes d'autorisation de mise en œuvre de dispositifs biométriques reposant sur l'empreinte digitale avec stockage dans une base de données.

A cet égard, la doctrine de la Commission, qui prend en considération les risques

liés à cette technologie au regard des droits et libertés consacrés par la loi du 6 janvier 1978 modifiée, considère le recours à de tels dispositifs comme justifiés uniquement s'ils sont fondés sur un fort impératif de sécurité.

En l'espèce, constatant l'absence de circonstances particulières attestant de la réalité d'un tel impératif, la formation plénière de la Commission a refusé d'accorder l'autorisation requise par la société C. pour mettre en œuvre le dispositif biométrique concerné. Cette délibération de refus a été notifiée à la société par lettre recommandée avec accusé de réception, reçue le 18 mai 2007.

Le contrôle sur place diligenté par la Commission le 28 février 2010

En application de la décision n° du 19 février 2010 du président de la Commission, une délégation de la CNIL a procédé à un contrôle sur place auprès de la société M. le 25 février 2010.

Ce contrôle avait notamment pour objet de vérifier si la société M. s'était conformée au refus d'autorisation prononcée par la CNIL le 25 avril 2007.

Lors de ce contrôle, les services de la Commission ont constaté que la société a mis en œuvre trois dispositifs biométriques : le premier au niveau de la porte d'entrée de la société, le deuxième au niveau de la porte d'accès aux bureaux, et le troisième à la porte de la salle informatique.

En premier lieu, les services de la Commission ont relevé que le premier de ces dispositifs biométriques, installé à la porte d'entrée du hall de l'entreprise, reposait sur la technologie du contour de la main. Ce dispositif était conforme aux dispositions de l'autorisation unique AU-07 adoptée par la Commission le 27 avril 2006. La société a par ailleurs régulièrement fait l'objet d'un engagement de conformité à cette autorisation unique, selon les procédures en vigueur (déclaration n° . en date du 18 mars 2008).

En revanche, les services de la Commission ont constaté que tant le dispositif en place au niveau de la porte intérieure d'accès aux locaux administratifs que le dispositif en place au niveau de la porte d'accès à la salle des serveurs reposaient, l'un comme l'autre, sur le stockage en base centrale des empreintes digitales des salariés concernés. Ces constatations ont permis d'établir que la société M. n'avait pas tenu compte du refus d'autorisation émis par la Commission le 25 avril 2007, soit plus de trois ans après la notification de celle-ci.

Lors de sa présence dans les lieux, la délégation de la Commission a également constaté la société n'avait pas fourni aux salariés concernés d'information sur les droits qui leur sont garantis par la loi « Informatique et Libertés ».

Elle a également constaté qu'aucune durée de conservation n'avait été définie pour les données de passage, contrairement aux gabarits biométriques et aux données d'identification, dont il est prévu qu'elles soient conservées jusqu'au départ du salarié.

B. Procédure

A la suite de ce contrôle, il a été décidé d'engager une procédure sur le fondement du 1° du II de l'article 45 de la loi du 6 janvier 1978 modifiée.

A cette fin, le rapport de M. Jean MASSOT, rapporteur, proposant à la formation restreinte de la CNIL de prononcer une mesure d'interruption du traitement de gestion du contrôle de l'accès aux locaux reposant sur l'empreinte digitale mis en œuvre par la société M. , a été notifiée par huissier à la société le 2 mars 2010.

Le 1° du II de l'article 45 de la loi du 6 janvier 1978 modifiée dispose :

« En cas d'urgence, lorsque la mise en œuvre d'un traitement ou l'exploitation des données traitées entraîne une violation des droits et libertés mentionnés à l'article 1er, la Commission peut, après une procédure contradictoire :

1° Décider l'interruption de la mise en œuvre du traitement, pour une durée maximale de trois mois, si le traitement n'est pas au nombre de ceux qui sont mentionnés au I de l'article 26 ou de ceux mentionnés à l'article 27 mis en œuvre par l'Etat ».

La société M. étant une société de droit privé, les exceptions précitées ne lui

La société M. étant une société de droit privé, les exceptions précitées ne lui sont pas applicables. La Commission est dès lors fondée à envisager de lui appliquer la mesure d'interruption prévue à l'article ci-dessus.

Au soutien de sa demande et au vu des constats précités, le rapporteur a fait valoir l'urgence qui caractérise la situation, en rappelant que, s'agissant de la défense de libertés individuelles, il n'est pas besoin de constater péril imminent ou dommages irréparables et irréversibles pour juger de l'application de cette notion.

En outre, le rapporteur a relevé les éléments suivants pour caractériser les manquements à la loi du 6 janvier 1978 modifiée :

En premier lieu, la mise en place induite d'un traitement que la société M. savait illégal depuis la notification du refus, le 18 mai 2007. Pour qualifier la gravité de ce manquement, le rapporteur rappelle que le régime de demande d'autorisation s'applique aux traitements les plus sensibles en termes de risque d'atteinte aux droits et libertés protégés par la loi du 6 janvier 1978 modifiée. En outrepassant la décision de la CNIL, la société a ainsi laissé fonctionner un traitement de nature à porter gravement atteinte à la vie privée, et ce jusqu'au jour de son constat sur place par la Commission. De tels faits sont de nature à contrevenir aux dispositions de l'article 25 de la loi du 6 janvier 1978 modifiée, ainsi qu'à celles de l'article 226-16 du Code pénal, qui prévoit que « le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en œuvre prévues par la loi est puni de cinq ans d'emprisonnement et de 300 000 € d'amende ».

En second lieu, le défaut d'information des salariés concernés sur l'existence et les caractéristiques du traitement, alors que la société précisait dans sa demande d'autorisation qu'elle procéderait à leur information par une note d'information (dossier n°). La délégation de la CNIL a au contraire constaté que les salariés n'avaient reçu aucune information sur les caractéristiques de ce traitement, et en particulier sur les droits qu'ils détiennent en application de la loi « informatique et libertés ». De tels faits sont de nature à contrevenir aux dispositions du I de l'article 32 de la loi du 6 janvier 1978 modifiée, et notamment son 6°, qui prévoit que « la personne auprès de laquelle sont recueillies des données à caractère personnel la concernant est informée, sauf si elle l'a été au préalable, par le responsable du traitement ou son représentant (...) des droits qu'elle tient des dispositions de la section 2 du présent chapitre », y compris l'identité de la personne auprès de laquelle exercer leurs droits ;

En troisième lieu, l'absence de limitation des données de passage stockées par le dispositif, alors que la société précisait dans sa demande d'autorisation qu'elle procéderait à leur effacement dans un délai de deux mois à compter de leur enregistrement. La délégation de la CNIL a au contraire constaté que la société disposait de données de passage datant de juin 2006 à mars 2008, et que la seule raison pour laquelle cet enregistrement ne s'est pas poursuivi au-delà de mars 2008 tient à la capacité de stockage du traitement qui, une fois atteinte, n'a pas permis d'enregistrer de nouvelles données. Le rapporteur relève sur ce point que la conservation illimitée des données de passage enregistrées constitue une atteinte grave à la vie privée des personnes concernées, et que de tels faits sont de nature à contrevenir aux dispositions de l'article 6 de la loi du 6 janvier 1978 modifiée, et notamment son 5°, qui prévoit que « un traitement ne peut porter que sur des données à caractère personnel qui satisfont aux conditions suivantes : (...) 5° elles sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées ».

Par une télécopie en date du 17 mars 2010, la société M. a adressé à la Commission ses observations sur le rapport.

Cette télécopie fournit en premier lieu un historique de la société et de ses changements d'actionariat, la chronologie de ces modifications sociales justifiant, selon elle, que la nouvelle équipe de direction de la société ne pouvait être informée du refus de la Commission en date du 18 mai 2007.

Elle souligne également la nature spécifique de ses activités. De fait, selon Mme D., les activités de la société sont « sous douane ». C'est en raison de ce statut spécifique, qui s'attache à la nature de la marchandise commercialisée par la

spécifique, qui s'attache à la nature de la marchandise commercialisée par la société M. , que celle-ci a mis en place le dispositif biométrique mis en cause. L'installation de ce dispositif aurait résulté des exigences de l'administration des Douanes et des assureurs de la société.

Par ailleurs, le courrier de la société M. fournit un récapitulatif des actions entreprises depuis la mission de contrôle diligentée par la Commission dans ses locaux, notamment :

la rédaction d'une note d'information ayant vocation à être communiquée aux personnes concernées pour les informer des droits qu'ils détiennent en application de la loi « informatique et libertés »,

un devis visant à remplacer les systèmes reposant sur l'empreinte digitale des bureaux et du serveur,

une copie de l'effacement des données de passage.

Ces actions tendent, selon la société M., à démontrer sa bonne foi et le souci de régulariser sa situation auprès de la Commission.

Lors de la séance de la formation restreinte de la CNIL du 18 mars 2010, Mme D. , gérante, et M. O., responsable administratif et financier, ont également présenté leurs observations orales.

Sans nullement contester la matérialité des faits, les représentants de la société ont de nouveau exposé à la Commission les mesures prises en vue de régulariser leur situation. Il est apparu lors des débats que le dispositif mis en cause était à ce jour encore opérationnel.

Motifs de la décision

Sur l'urgence à interrompre la mise en œuvre du traitement de gestion du contrôle de l'accès aux locaux, reposant sur l'empreinte digitale

Sans qu'il y ait nécessairement péril imminent ou dommages irréparables et irréversibles, l'urgence est caractérisée dès lors qu'une circonstance est susceptible d'entraîner, s'il n'y est porté remède à bref délai, un préjudice grave et immédiat aux droits et libertés mentionnés à l'article 1er de la loi du 6 janvier 1978 modifiée. Une telle situation d'urgence s'apprécie au regard des intérêts qui sont en cause, de la gravité de leur atteinte ainsi que du nombre de personnes concernées.

Relevant la gravité des manquements constatés lors de la mission de contrôle, et notamment la mise en œuvre persistante par la société M. d'un dispositif biométrique ayant fait l'objet d'un refus d'autorisation, lequel était encore en place au jour de l'audience, la Commission considère dès lors que la condition d'urgence requise par le 1° du I de l'article 45 est qualifiée dans les faits, et qu'il lui appartient dès lors d'agir sans délai pour la conservation d'un droit ou la sauvegarde des libertés consacrées par la loi « informatique et libertés ».

Sur la violation des droits et libertés mentionnés à l'article 1er de la loi du 6 janvier 1978 modifiée

La Commission rappelle que la délégation de la CNIL a, lors du contrôle du 25 février 2010, constaté que la société mettait en œuvre un traitement de gestion du contrôle de l'accès aux locaux reposant sur l'empreinte digitale, et ce malgré sa décision explicite de refus en date du 25 avril 2007.

Elle retient que la société a ainsi indûment mis en place un traitement qu'elle savait illégal depuis la notification du refus, le 18 mai 2007, étant rappelé que le régime de demande d'autorisation s'applique aux traitements les plus sensibles en termes de risque d'atteinte aux droits et libertés protégés par la loi du 6 janvier 1978 modifiée. En outrepassant la décision de la Commission, la société a ainsi laissé fonctionner un traitement de nature à porter gravement atteinte à la vie privée des personnes concernées, et ce jusqu'au jour de son constat sur place par la Commission.

En outre, elle constate que les deux dispositifs biométriques mis en cause visent à contrôler l'accès des personnes d'une part à un local informatique, et d'autre part la porte d'accès aux bureaux. La Commission s'interroge dès lors sur la

part la porte d'accès aux bureaux. La Commission s'interroge sur la pertinence de l'argument selon lequel l'installation de ces lecteurs biométriques aurait résulté des exigences de l'administration des Douanes et des assureurs de la société, dans la mesure où ces dispositifs ne viseraient dès lors pas à protéger des marchandises. En tout état de cause, il ne peut être pris appui sur ces exigences pour justifier de la mise en place d'un dispositif illégal, quand des dispositifs alternatifs, compatibles avec la doctrine de la Commission, auraient aussi bien permis de satisfaire à de telles obligations réglementaires et contractuelles.

Par ailleurs, la société indique qu'elle a pris des mesures de nature à se conformer aux décisions et constats de la Commission depuis son contrôle.

Sur ce point, en premier lieu, la Commission prend acte du fait que la société M. a rédigé une note d'information à destination de son personnel. Si la Commission considère ce premier élément comme satisfaisant, elle note toutefois qu'il ne ressort pas des écritures de la société que cette information a été effectivement communiquée aux personnes concernées.

En second lieu, la Commission prend également acte du fait que la société M. a effacé les données de passage du système de stockage. Si cet élément doit également être tenu pour satisfaisant, la Commission note toutefois que cette mesure ponctuelle et transitoire ne saurait équivaloir à la mise d'une politique de purge, assortie des procédures et moyens techniques correspondants, qui seraient seuls de nature à la mettre en mesure de satisfaire à ses obligations au regard de la loi du 6 janvier 1978 modifiée.

Dès lors, la Commission se doit de relever que, pour l'heure, elle ne dispose d'aucun élément concret susceptible de la faire conclure à la cessation des manquements constatés, et dès lors à modifier son appréciation sur les faits l'ayant conduit à faire examiner ce dossier par la formation restreinte.

C'est pourquoi, eu égard à la gravité des manquements constatés, au surplus réitérés lors de l'audience, la Commission ne saurait trouver aucune justification au maintien de cette situation, s'agissant en particulier de la mise en œuvre persistante d'un traitement ayant fait l'objet d'un refus d'autorisation de sa part.

PAR CES MOTIFS

Conformément au 1° du II de l'article 45 de la loi du 6 janvier 1978 modifiée, la formation restreinte de la CNIL, après en avoir délibéré, décide :

D'ordonner l'interruption du traitement déclaré à la Commission sous le numéro. pour une durée de trois mois à compter de la notification de la présente décision, délai durant lequel il lui appartiendra de se mettre en conformité avec les dispositions de la loi du 6 janvier 1978 modifiée.

La société M. dispose d'un délai de deux mois pour exercer un recours devant le Conseil d'Etat à l'encontre de la présente délibération.

Le Président Alex TÜRK