Délibération de la formation restreinte n°2014-261 du 26 juin 2014 prononçant un avertissement rendu public à l'encontre de la société X

Séquestration et privation de liberté en contexte sectaire | Délibérations CNIL | En vigueur

Date	12/07/2014
Juridiction / Nature	deliberation
URL Légifrance	https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000029224324

RÉSUMÉ OFFICIEL LÉGIFRANCE

[...] Des droits qu'elle tient des dispositions de la section 2 du présent chapitre ; 7° Le cas échéant, des transferts de données à caractère personnel envisagés à destination d'un Etat non membre de la Communauté [...] Si ces exigences ont finalement été respectées par la mise en place d'un accès https, force est de constater que cette mise en conformité ne découle que de l'initiation d'une procédure de sanction, puisque [...]

TEXTE INTÉGRAL

La Commission nationale de l'informatique et des libertés, réunie en sa formation restreinte composée de M. Jean-François CARREZ, Président, de M. Alexandre LINDEN, Vice-président, Mme Marie-Hélène MITJAVILE, M. Sébastien HUYGUES et M. Maurice RONAI, 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° 2011-334 du 29 mars 2011, notamment ses articles 45 et 46 ; 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° 2013-175 du 4 juillet 2013 portant adoption du règlement intérieur de la Commission nationale de l'informatique et des libertés ;Vu la décision n° 2011-253C du 21 septembre 2011 de la Présidente de la Commission nationale de l'informatique et des libertés ordonnant une mission de vérification auprès de la société X ;Vu la décision de la Présidente de la Commission portant désignation d'un rapporteur, en date du 25 février 2014;Vu le rapport de M. François PELLEGRINI, commissaire rapporteur, adressé par porteur à la société X, le 11 mars 2014; Vu les observations écrites versées par la société X, complétées par les observations orales formulées lors de la séance de la formation restreinte;Vu le courrier d'observation parvenu à la formation restreinte postérieurement à l'audience, le 18 avril 2014 ; Vu les autres pièces du dossier ;Ayant entendu, lors de la séance de la formation restreinte du 17 avril 2014 se tenant à huis clos, à la demande de la société :- M. François PELLEGRINI, commissaire rapporteur, en son rapport ;- Mme Catherine POZZO DI BORGO, commissaire du Gouvernement adjoint, en ses observations ;- M. X, de la société X et M. Y, de la société, assistés de Maître Z, avocate,A adopté la décision suivante : I. FAITS ET PROCÉDURELa société X (ci-après la société) propose un service de suivi de régime en ligne selon la méthode d'amaigrissement développée par le Dr XX.Elle propose aux internautes de s'inscrire, via son site Internet, à un programme personnalisé comportant des conseils adaptés à leurs profils alimentaires, une messagerie privée permettant d'échanger avec une diététicienne, une plateforme de chat et un forum ou encore des vidéos d'exercice physique.A l'occasion d'un contrôle diligenté dans les locaux de la société le 22 septembre 2011, les services de la Commission se sont attachés à vérifier la conformité des traitements de données à caractère personnel mis en œuvre par la

société à la loi n°78-17 du 6 janvier 1978 modifiée, notamment ceux issus du site Internet [...]. Un deuxième contrôle a été diligenté le 11 octobre 2011 afin de permettre aux services de la Commission de vérifier de manière spécifique les aspects techniques des traitements de données à caractère personnel opérés par la société à travers ce site. Suite à ces deux contrôles, plusieurs demandes complémentaires ont été adressées à la société dans le but de vérifier qu'elle mettait en œuvre un niveau suffisant de sécurité et de confidentialité des données collectées auprès de ses clients. Compte tenu des réponses tardives de la société, un nouveau contrôle a été diligenté le 17 septembre 2013 afin de s'assurer de la mise en œuvre des mesures correctives annoncées. A l'issue des échanges s'étant ensuivis, considérant que les réponses de la société n'étaient pas satisfaisantes, la Présidente de la Commission a décidé d'initier une procédure de sanction à l'encontre de la société. A cet effet, elle a désigné M. François PELLEGRINI en qualité de rapporteur, le 25 février 2014, sur le fondement de l'article 46 de la loi du 6 janvier 1978 modifiée. A l'issue de son instruction, considérant que la société avait manqué à plusieurs obligations lui incombant en application de la loi du 6 janvier 1978 modifiée, le rapporteur a notifié à la société, le 11 mars 2014, un rapport détaillant les manquements à la loi qu'il estimait constitués en l'espèce. Au vu de ceux-ci, le rapporteur a par ailleurs proposé à la formation restreinte de la Commission de prononcer à son encontre un avertissement, dont il sollicitait par ailleurs qu'il soit rendu public. Était également jointe au rapport une convocation à la séance de la formation restreinte du 17 avril 2014 indiquant à la société qu'elle disposait d'un délai d'un mois pour communiquer ses observations écrites. La société a produit, par courrier daté du 11 avril 2014, des observations écrites sur le rapport, réitérées oralement lors de la séance de la formation restreinte tenue à huis-clos le 17 avril 2014.Par un courrier du 18 avril 2014, la société a par ailleurs adressé à la formation restreinte, au rapporteur et aux services de la Commission des éléments complémentaires à ceux développés lors de l'audience, afin d'attester de la mise en œuvre de certaines mesures de sécurité annoncées oralement. Au vu de ces éléments, et après en avoir délibéré, la formation restreinte a adopté la décision dont la teneur suit. II. MOTIFS DE LA DÉCISION1. Sur le manquement à l'obligation d'informer les personnesL'article 32-I de la loi n° 78-17 du 6 janvier 1978 modifiée dispose 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 : 1° De l'identité du responsable du traitement et,

le cas échéant, de celle de son représentant ; 2° De la finalité poursuivie par le traitement auquel les données sont destinées ; 3° Du caractère obligatoire ou facultatif des réponses ; 4° Des conséquences éventuelles, à son égard, d'un défaut de réponse ; 5° Des destinataires ou catégories de destinataires des données ; 6° Des droits qu'elle tient des dispositions de la section 2 du présent chapitre ; 7° Le cas échéant, des transferts de données à caractère personnel envisagés à destination d'un Etat non membre de la Communauté européenne. Lorsque de telles données sont recueillies par voie de questionnaires, ceux-ci doivent porter mention des prescriptions figurant aux 1°, 2°, 3° et 6°. Les deux contrôles sur place opérés les 22 septembre et 11 octobre 2011 ont permis de constater que la société ne faisait pas figurer sur les divers supports de collecte de données à caractère personnel de son site Internet les mentions d'information prévues par les dispositions de cet article. Le 3 juillet 2012, soit près de neuf mois après ce second contrôle, la société a indiqué à la CNIL avoir fait le nécessaire pour procéder à bref délai à l'insertion de ces mentions sur l'ensemble de ces formulaires, notamment en ayant fait rédiger la clause appelée à être insérée sur les documents par la personne en charge en charge des affaires juridiques jusqu'en 2012. Pour autant, lors du troisième contrôle opéré le 17 septembre 2013, la Commission a constaté que ces mentions faisaient toujours défaut sur plusieurs formulaires de collecte. La société s'est justifiée sur ce point en invoquant de nombreux mouvements de membres de ses équipes occupant des postes clés, puis un changement de direction à sa tête au mois de juin 2013 qui l'aurait mise dans l'impossibilité de mobiliser ses équipes sur la question de la protection des données personnelles et de répondre dans des délais raisonnables aux sollicitations de la Commission. En tout état de cause, elle a soutenu dans ses observations en défense que les mentions légales requises ont finalement été portées sur les différents formulaires mis en ligne sur son site internet. La formation restreinte admet que ce manquement avait été résolu au jour de l'audience, tout en relevant que le bénéfice de cette mise en conformité ne pouvait être imputé qu'à la procédure de sanction initiée à l'encontre de la société. Elle constate, à cet égard, que celle-ci n'a pas respecté ses obligations pendant plus de deux ans alors même que, comme elle l'admet dans ses écritures, cette insertion ne présentait aucune difficulté technique ni aucun coût de mise en œuvre particulier et que la Commission avait mis cette déficience en évidence lors de deux contrôles. 2. Sur le manquement à l'obligation d'assurer la sécurité et la confidentialité des donnéesL'article 34 de la loi du 6 janvier 1978 modifiée dispose que Le responsable du traitement

est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès .Il appartient à la formation restreinte de décider si la société a manqué à l'obligation lui incombant de mettre en œuvre des moyens propres à assurer la sécurité des données de ses clients, notamment afin que ces données ne soient pas communiquées à des tiers non autorisés. Cette exigence de sécurité doit s'apprécier notamment au regard du fait que les données communiquées par ses clients et prospects à la société relèvent pour une large part de l'intimité de ceux-ci (historique de poids, nombre de grossesses, habitudes alimentaires, composition du foyer, consommation d'alcool, pratiques sportives etc.), et revêtent donc une réelle sensibilité.A cet égard, les faits pertinents de l'affaire sont les suivants.En premier lieu, les contrôles diligentés par la Commission ont permis d'établir, dès l'année 2011, que la connexion aux outils de gestion du site litigieux ainsi qu'à l'administration de la base regroupant les données clients et prospects s'effectuait dans des conditions ne permettant pas d'assurer un niveau de sécurité satisfaisant. Il est constant que des mesures de sécurisation des accès ont bien été mises en œuvre dès la réalisation de ces premiers contrôles. En revanche, la société ne s'est pas mise en mesure de respecter les exigences relatives à la sécurisation des flux entre le poste de la personne et le serveur sur lequel elle se connecte, alors pourtant que celles-ci avaient été formulées dès l'année 2012. Si ces exigences ont finalement été respectées par la mise en place d'un accès https, force est de constater que cette mise en conformité ne découle que de l'initiation d'une procédure de sanction, puisque la mise en place de cette mesure n'a été confirmée que par les observations parvenues à la Commission le 18 avril 2014, soit le lendemain de l'audience s'étant déroulée devant la formation restreinte dans le cadre du présent litige. Par ailleurs, les contrôles effectués en 2011 ont permis d'établir que la société conservait les mots de passe de ses clients et prospects en clair dans sa base de données dédiée, soit environ 6 millions d'utilisateurs. Au jour de l'audience, il a été acté que la société avait procédé au chiffrement de l'intégralité de ces mots de passe. Cependant, il importe de relever que le contrôle préalablement effectué le 22 septembre 2013 avait permis de constater que les mots de passe relatifs aux comptes clients (par opposition aux comptes prospects) étaient alors toujours conservés en clair dans la base de données, contrairement aux assurances données en sens contraire à la Commission le 2 juillet 2012. Enfin, les premiers contrôles ont mis en évidence que si

le formulaire de paiement en ligne était chiffré de manière satisfaisante, des données à caractère personnel étaient en revanche collectées sur d'autres formulaires du site sans sécurisation. Ici encore, la société a indiqué qu'elle étendrait le protocole https aux données transmises par les formulaires concernés, mais la mission de contrôle effectuée en septembre 2013 a permis de constater que la société n'avait pas mis en œuvre la mesure corrective annoncée en 2012. La société se défend sur l'ensemble de ces dysfonctionnements en invoquant les multiples réorganisations ayant été subies par ses équipes, ainsi qu'une fusion opérée en novembre 2013 ayant profondément déstabilisé son organisation. Elle invoque également une campagne de diffamation initiée à son encontre qui aurait pour but de provoquer sa désorganisation en interne autant qu'auprès de l'opinion publique. Elle soutient avoir finalement satisfait à l'ensemble des demandes formulées par la Commission en matière de sécurité informatique et, en tout état de cause, n'avoir subi aucune atteinte aux données qu'elle traite. Au vu de ce qui précède, la formation restreinte considère ce qui suit. La société X met aujourd'hui en œuvre un niveau de sécurité suffisant pour les données à caractère personnel qu'elle collecte à travers son site Internet. Il est certain, par ailleurs, que l'ensemble des dysfonctionnements constatés ne peuvent sans doute pas être directement imputés aux responsables actuels de la société, celle-ci ayant été manifestement perturbée par les changements réguliers de ses dirigeants et personnels, notamment de son responsable de la sécurité informatique et de son responsable juridique. Néanmoins, au vu des éléments rapportés ci-dessus, il n'est pas davantage contestable que la société a mis plus de trois ans à appliquer un niveau de sécurité satisfaisant aux données personnelles qu'elle collecte à travers son site internet. Ce défaut de mise en conformité doit être analysé au regard du fait que la Commission a fait part de ces exigences à plusieurs reprises, à l'occasion de trois contrôles sur place ainsi qu'au travers d'une correspondance nourrie visant à permettre à la société de respecter les exigences de sécurité qui lui incombaient, et ce avant même toute initiation de procédure contentieuse. Compte tenu du nombre et de la nature des informations collectées à travers le site internet [...], une attention toute particulière devait être apportée au maintien de leur sécurité et de leur confidentialité. Il est incontestable que cette attention a fait défaut pendant plusieurs années, alors même que la société avait été précisément informée de la nature des mesures devant être mises en œuvre à cet effet, et quand bien même elle s'est in fine mise en conformité à cet égard. Dans ces conditions, la formation restreinte

constate que la société n'a pas respecté les dispositions de l'article 34 de la loi du 6 janvier 1978 modifiée sur une période substantielle. Elle estime par conséquent que ce manquement est constitué. 3. Sur le manquement à l'obligation de confidentialité des données gérées par un sous-traitantL'article 35 de la loi n° 78-17 du 6 janvier 1978 modifiée dispose : Les données à caractère personnel ne peuvent faire l'objet d'une opération de traitement de la part d'un sous-traitant, d'une personne agissant sous l'autorité du responsable du traitement ou de celle du sous-traitant, que sur instruction du responsable du traitement. Toute personne traitant des données à caractère personnel pour le compte du responsable du traitement est considérée comme un sous-traitant au sens de la présente loi. Le sous-traitant doit présenter des garanties suffisantes pour assurer la mise en œuvre des mesures de sécurité et de confidentialité mentionnées à l'article 34. Cette exigence ne décharge pas le responsable du traitement de son obligation de veiller au respect de ces mesures. Le contrat liant le sous-traitant au responsable du traitement comporte l'indication des obligations incombant au sous-traitant en matière de protection de la sécurité et de la confidentialité des données et prévoit que le sous-traitant ne peut agir que sur instruction du responsable du traitement. Il appartient à la formation restreinte de décider si la société a manqué à l'obligation lui incombant en application des dispositions ci-dessus en n'insérant pas de clause destinée à assurer la confidentialité des données personnelles des utilisateurs de son site Internet.A cet égard, les faits pertinents de l'affaire sont les suivants.Lors des contrôles opérés en 2011, la Commission a constaté que le contrat conclu par la société avec un prestataire de campagnes d'emailing ne comportait pas de clause spécifique à cet effet. Si une clause de confidentialité figurait alors au contrat, celle-ci ne visait cependant qu'à protéger les informations de nature commerciale, financière ou relevant des méthodes et savoir-faire du prestataire. Il a donc été demandé à la société d'insérer des clauses de sécurité ad hoc, relatives à la protection des données personnelles de ses clients. Sur ce point, la formation restreinte relève que le contrat de prestation de service en vigueur depuis le 18 octobre 2012 comporte effectivement, comme l'invoque la société dans ses écritures, une clause intitulée Sécurité des données et des échanges qui a trait, entre autres et de manière spécifique, à la protection de ces données. De fait, si la précédente version du contrat ne comportait pas une telle stipulation, celui-ci n'était plus en vigueur depuis cette date. Par ailleurs, un avenant a été signé avec l'autre de ses prestataires, en 2012, suite à la demande formulée par la Commission en ce sens.La formation restreinte retient,

dans ces conditions, que les faits de l'affaire ne sont pas de nature à qualifier l'existence d'un manquement à l'article 35 de la loi du 6 janvier 1978 modifiée. 4. Sur le manquement à l'obligation de coopération avec la CommissionL'article 21 de la loi n° 78-17 du 6 janvier 1978 modifiée dispose : Dans l'exercice de leurs attributions, les membres de la commission ne reçoivent d'instruction d'aucune autorité. Les ministres, autorités publiques, dirigeants d'entreprises publiques ou privées, responsables de groupements divers et plus généralement les détenteurs ou utilisateurs de traitements ou de fichiers de données à caractère personnel ne peuvent s'opposer à l'action de la commission ou de ses membres et doivent au contraire prendre toutes mesures utiles afin de faciliter sa tâche. Sauf dans les cas où elles sont astreintes au secret professionnel, les personnes interrogées dans le cadre des vérifications faites par la commission en application du f du 2° de l'article 11 sont tenues de fournir les renseignements demandés par celle-ci pour l'exercice de ses missions. Il appartient à la formation restreinte de décider si la société a manqué à l'obligation de coopération avec la Commission consacrée par cette disposition dans cette affaire.A cet égard, les faits pertinents sont les suivants.En diligentant les contrôles des 21 septembre et 11 octobre 2011, la Commission a engagé auprès de la société une démarche visant à l'accompagner vers une mise en conformité de ses traitements de données à caractère personnel portant sur ses clients. Les réponses apportées par cette dernière lors des échanges s'étant ensuivis ont assuré la Commission de la prise de mesures correctives à l'ensemble des manquements relevés. Or, le contrôle du 17 septembre 2013 a révélé que la société n'avait pas satisfait aux demandes de la Commission sur de nombreux points. Il a par ailleurs fallu que de très nombreux échanges s'ensuivent pour parvenir à obtenir la mise en œuvre de garanties de sécurité fondamentales, telles que l'extension du protocole https à l'ensemble des transmissions de données effectuées à travers les formulaires accessibles sur le site de la société. De même, celle-ci n'a pas fourni d'information complète aux personnes sur les formulaires de collecte accessibles sur son site Internet pendant plus de deux ans, soit depuis le déroulement des contrôlées opérés en 2011, alors pourtant qu'aucune difficulté technique ou charge financière particulière ne s'opposait à une mise en conformité rapide, et alors même, comme la société l'a indiqué dans ses écritures, qu'un modèle de clause avait été rédigé à cet effet par la personne en charge des affaires juridiques dans l'entreprise. Par ailleurs, plus de deux ans après le premier contrôle, le projet de charte informatique engagé n'avait pas été achevé, ni aucune procédure mise en œuvre aux fins de purge

des données conservées. Il résulte de ce qui précède que si la société n'a pas délibérément cherché à tromper la Commission sur les mesures prétendument mises en œuvre, elle a à tout le moins agi avec une indéniable légèreté qui, si elle ne peut être entièrement imputable aux dirigeants actuels de la société, constitue cependant un manquement à l'article 21 susvisé. 5. Sur la sanction et la publicitéLa formation restreinte constate que la société n'a pas respecté les dispositions prévues aux articles 34 et 21 de la loi n°78-17 du 6 janvier 1978 modifiée. Par conséquent, elle décide de prononcer à son encontre la sanction de l'avertissement prévu à l'article 45 de la loi n°78-17 du 6 janvier 1978 modifiée. Par ailleurs, au regard du nombre de personnes concernées, de la sensibilité des données concernées par les traitements litigieux et de la difficulté rencontrée par la Commission pour obtenir de la société une mise en conformité effective à la loi du 6 janvier 1978 modifiée, la formation restreinte décide de rendre cette décision publique. PAR CES MOTIFS La formation restreinte de la CNIL, après en avoir délibéré, décide : - De prononcer un avertissement à l'encontre de la société X - De rendre publique sa décision sur le site Internet de la CNIL et sur le site Légifrance. Le Président Jean-François CARREZ Cette décision est susceptible de faire l'objet d'un recours devant le Conseil d'Etat dans un délai de deux mois à compter de sa notification.

RÉFÉRENCE

deliberation du 12 juillet 2014, « Délibération de la formation restreinte n°2014-261 du 26 juin 2014 prononçant un avertissement rendu public à l’encontre de la société X ». Disponible sur Légifrance : https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000029224324 (consulté le 30 août 2026).