Date de publication sur legifrance: 02/08/2018

Commission Nationale de l'Informatique et des Libertés

Délibération n°SAN-2018-008 du 24 juillet 2018
Délibération de la formation restreinte n° SAN-2018-008 du 24 juillet 2018 prononçant une sanction pécuniaire à l'encontre de la société DAILYMOTION

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 Dominique CASTERA et Monsieur 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 suivants ;
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° 2016-357C du 8 décembre 2016 de la Présidente de la Commission nationale de l'informatique et des libertés de charger le secrétaire général de procéder ou de faire procéder à une mission de vérification auprès de la société DAILYMOTION :
Vu la décision de la Présidente de la Commission nationale de l'informatique et des libertés portant désignation d'un rapporteur devant la formation restreinte, en date du 9 mai 2017 ;
Vu le rapport de M. François PELLEGRINI, commissaire rapporteur, notifié à la société DAILYMOTION le 24 avril 2018 ;
Vu la demande de huis clos présentée par la société DAILYMOTION le 5 juin 2018 à laquelle, par courrier du 11 juin 2018, il n'a pas été fait droit ;
Vu les observations écrites de la société DAILYMOTION reçues le 5 juin 2018, ainsi que les observations orales formulées lors de la séance de la formation restreinte ;
Vu les autres pièces du dossier ;

Etaient présents, lors de la séance de la formation restreinte du 14 juin 2018 :
· M. François PELLEGRINI, Commissaire, en son rapport ;
En qualité de représentants de la société DAILYMOTION :
· […] ;
· […] ;
· […] ;

En qualité de conseil de la société DAILYMOTION :
· […] ;
· […].

Mme Nacima BELKACEM, Commissaire du Gouvernement, n'ayant pas formulé d'observations ;

Les représentants de la société DAILYMOTION ayant pris la parole en dernier ;

A adopté la décision suivante :

- Faits et procédure
- La procédure de contrôle sur place

La société DAILYMOTION (ci-après la société) est une société anonyme sise 140, Boulevard Malesherbes à PARIS (75017), qui propose une plateforme d'hébergement de contenus vidéo créés par des utilisateurs. Entre 260 et 300 millions d'utilisateurs se rendent sur cette plateforme chaque mois et les contenus mis en ligne bénéficient d'environ 3 milliards de vues mensuelles. En 2016, elle a réalisé un chiffre d'affaires de 58 809 200 euros.

Le 5 décembre 2016, un article publié sur le site web WWW.ZDNET.COM faisait état d'une fuite de plusieurs millions de données relatives à des adresses électroniques et des mots de passe d'utilisateurs de la plateforme de partage de vidéo de la société.

Le 15 décembre 2016, en application de la décision n°2017-357C de la Présidente de la Commission nationale de l'informatique et des libertés (ci-après la CNIL ou la Commission), une délégation de la Commission a procédé à une mission de contrôle au sein des locaux de la société.

A l'occasion de ce contrôle, la société a indiqué à la délégation qu'elle avait été alertée de l'existence de la violation de donnés par un courrier électronique adressé au Directeur général délégué de la société le 5 décembre 2016. Elle a également confirmé que la violation de données avait concerné 82,5 millions d'adresses de comptes ainsi que 18,3 millions de mots de passe chiffrés extraits des tables *user* (utilisateurs) et *user_password* (mot de passe des utilisateurs) de la base de données de la société.

La société a précisé qu'elle avait identifié la violation de données le 6 décembre 2016 à la suite de sa révélation par le site web WWW.ZDNET.COM . Elle a indiqué à la délégation que *l'attaque est due à l'exécution d'une requête SQL de type SELECT ; que cette requête a été exécutée sur les tables user et user_passwords ; que les données ont été récupérées sur une machine ayant une IP située sur le territoire américain ;*

[…]

La société a également indiqué que compte tenu de ce que le volume de données téléchargées était faible en proportion des capacités de la bande passante, aucune alerte n'avait été remontée lors de l'extraction de données. Elle a précisé qu'en réaction à cette attaque, elle avait immédiatement mis en place plusieurs mesures renforçant la sécurité de son système d'information, notamment […].

Il a été précisé à la délégation qu'elle n'avait pas mis en place de politique de mots de passe complexes pour des *raisons de marketing* et qu'en dehors des cas où une demande de suppression de compte est formulée, la durée de conservation des données des utilisateurs n'était pas limitée. La société a par ailleurs expliqué qu'elle utilisait les services de la plateforme […] afin d'améliorer la sécurité de ses traitements et que des audits de sécurité étaient réalisés tous les trimestres.

Enfin, la société a indiqué qu'elle n'avait pas été victime d'un chantage particulier lié à cette vulnérabilité, que la valeur sur internet de la base de données attaquée serait de 11 euros et que l'ensemble des utilisateurs avaient été informés de l'incident.

Aux fins d'instruction de ces éléments, la Présidente de la Commission a désigné M. François PELLEGRINI en qualité de rapporteur, le 9 mai 2017, sur le fondement de l'article 46 de la loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés (ci-après loi Informatique et Libertés ou loi du 6 janvier 1978 modifiée).

A l'issue de son instruction, le rapporteur a notifié à la société DAILYMOTION le 3 juillet 2017 un rapport détaillant les manquements à la loi qu'il estimait constitués en l'espèce et a proposé à la formation restreinte de prononcer une sanction pécuniaire de cinq cent mille (500.000) euros qui serait rendue publique. Ce rapport était accompagné d'une convocation pour la séance de la formation restreinte du 21 septembre 2017 et invitait la

société à produire des observations en réponse dans un délai courant jusqu'au 7 septembre 2017.
A la suite de la réception de ce rapport, la société a adressé des observations en réponse par courrier du 6 septembre 2017. Ces observations ont fait apparaître de nombreux éléments nouveaux quant au déroulement des faits reprochés, en particulier sur le fait que l'incident de sécurité ne serait pas le résultat d'une injection SQL, contrairement à ce qui avait pu être initialement indiqué à la délégation de contrôle.
Afin de lui permettre de diligenter des investigations complémentaires, le rapporteur a, le 18 septembre 2017, adressé une demande de report de séance au président de la formation restreinte, laquelle a été acceptée. La société a été informée de ce report par courrier du même jour.

· Les investigations complémentaires.

Dans le cadre de ses investigations complémentaires, le rapporteur a, le 26 octobre 2017, adressé à la société, un questionnaire relatif à la violation de données, auquel la société a répondu par courrier du 23 novembre 2017. Puis, le rapporteur a procédé à l'audition des représentants de la société dans les locaux de la CNIL le 15 février 2018.
Au cours de ces investigations, la société a expliqué que l'incident de sécurité résultait d'une attaque en plusieurs étapes, menée par des délinquants informatiques chevronnés , au terme d'une démarche coordonnée sur plusieurs mois et vraisemblablement par plusieurs personnes.
Elle a précisé que cette attaque était le résultat de la combinaison de six facteurs, à savoir :

· *un accès frauduleux au code source de la société ;*
· *l'identification d'un bug exploitable de manière malveillante au sein des centaines de milliers de lignes de code de la plateforme Dailymotion ;*
· *le développement d'une compréhension de l'architecture de la plateforme permettant d'identifier les conditions nécessaires et suffisantes à l'exploitation malveillante du bug ;*
· *le développement d'un code d'exploitation spécifique à même de déclencher et de tirer profit du bug ;*
· *la capacité de détourner un compte d'administration pour exploiter le bug identifié ;*
· *la propagation de l'intrusion depuis les serveurs web vers des données tout en masquant son identité réelle par un jeu de rebonds vers des serveurs loués spécifiquement à ces fins* .

La société a précisé que le code source stocké au sein de la plateforme Github contenait un compte de service disposant des privilèges d'administration et qu'il était utilisé pour effectuer des tests de non régression.
[…]
Enfin, elle a indiqué qu'à la date du 15 février 2018, aucun de ses usagers n'avait fait état d'un quelconque préjudice à la suite de l'incident de sécurité.
Au regard des informations fournies par la société au rapporteur, celui-ci a préparé un nouveau rapport, se substituant à son rapport initial, proposant à la formation restreinte de prononcer une sanction pécuniaire qui ne saurait être inférieure à cent mille (100.000) euros et qui serait rendue publique. Ce rapport a été notifié à la société le 25 avril 2018 et était accompagné d'une convocation à la séance de la formation restreinte du 14 juin 2018, indiquant à la société qu'elle disposait d'un délai d'un mois pour communiquer ses observations écrites.
Par courrier du 5 juin 2018, la société DAILYMOTION a produit des observations écrites sur le rapport, réitérées oralement lors de la séance de la formation restreinte du 14 juin 2018.

· Motifs de la décision

Sur le manquement à l'obligation d'assurer la sécurité et la confidentialité des données.

L'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 .*

A titre liminaire, la société expose que l'article 34 de la loi Informatique et Libertés précité met à la charge du responsable de traitement une obligation de moyen et non de résultat. Elle considère qu'en l'espèce, elle n'a commis aucun manquement à ses obligations dans la mesure où l'extraction frauduleuse des données dont elle a été victime ne résulte pas de l'insuffisance des mesures qu'elle aurait prises en matière de sécurité mais d'une attaque particulièrement sophistiquée. Elle considère que la lecture de l'article 34 faite par le rapporteur revient à rendre imputable à un responsable de traitement n'importe quelle violation de données à caractère personnel, quelles que soient les circonstances techniques dans lesquelles serait intervenue cette violation.

La formation restreinte considère que l'article 34 précité met à la charge du responsable de traitement de mettre en œuvre des moyens propres à assurer la sécurité des données à caractère personnel contenues dans son système d'information et en particulier celles concernant les utilisateurs de sa plateforme web, notamment afin que ces données ne soient pas accessibles à des tiers non autorisés.

Il appartient donc à la formation restreinte de décider si la société DAILYMOTION a manqué à l'obligation lui incombant de prendre des mesures suffisantes.

Tout d'abord, s'agissant de la présence du mot de passe au sein du code source, la société explique que celui-ci est relatif à un compte de service aux fonctions particulières. La société a indiqué que ce compte de service avait pour objectif de simuler un administrateur afin de tester la validité des fonctionnalités d'administration. Elle explique que ces tests n'auraient pas été possibles en inscrivant le mot de passe dans le code source sous une forme hashée, car il faut nécessairement que le mot de passe soit inscrit en clair dans le code source pour que le compte de service puisse se connecter. Elle considère donc que la présence de ce mot de passe dans le code source n'est pas contraire à l'état de l'art.

La formation restreinte estime qu'en matière d'authentification, il est important de veiller à ce qu'un mot de passe permettant de s'authentifier sur un système ne puisse pas être divulgué. Ainsi, il est impératif qu'il ne soit pas stocké dans un fichier qui ne serait pas protégé.

S'il était nécessaire, pour le bon déroulement de tests relatifs au compte de service, que le mot de passe associé à ce compte soit inscrit en clair dans le code source, cette circonstance ne saurait toutefois, justifier, selon la formation restreinte, la présence constante du mot de passe dans le code source. Dans la mesure où il était impossible pour la société de conserver le mot de passe dans le code source sous une forme hashée, il lui revenait de chercher une autre solution afin de ne pas le rendre accessible, par exemple, en le stockant au sein de son réseau interne et en s'assurant qu'il était injecté en temps réel dans le code source, uniquement lors des phases de test puis supprimé une fois le test achevé.

Ensuite, s'agissant de l'absence de mesure de limitation des accès externes à l'administration du système d'information, la société explique que dès sa création, la plateforme DailyMotion a été conçue pour permettre à des utilisateurs extérieurs au réseau interne, en l'occurrence des partenaires de la société, de disposer de droit d'administration afin de pouvoir ajouter ou supprimer du contenu. A cet égard, la société a indiqué que les données extraites de son serveur ont été transmises vers un serveur extérieur ayant une adresse IP située sur le territoire des États-Unis d'Amérique.

La formation restreinte considère que lorsque des collaborateurs sont amenés à se connecter à distance au réseau informatique interne d'une entreprise, la sécurisation de cette connexion constitue une précaution élémentaire afin de préserver l'intégrité dudit réseau. Cette sécurisation peut, par exemple, reposer *a minima* sur la mise en place d'une mesure de filtrage des adresses IP afin que seules soient exécutées des requêtes provenant d'adresses IP identifiées et autorisées ou par l'utilisation d'un VPN, qui permet d'éviter toute connexion illicite, en sécurisant les échanges de données et en authentifiant les utilisateurs.
La formation restreinte relève qu'en l'espèce, la société a déployé une mesure de sécurisation des accès à son système d'information après la découverte de l'attaque […]. Or, la mise en place de cette mesure dès la conception de la plateforme aurait empêché l'attaquant d'avoir accès à l'interface d'administration depuis Internet.
Si la formation restreinte admet que la réussite de l'attaque résulte bien de la conjonction de plusieurs facteurs dont certains ne sont pas imputables à la société, elle considère toutefois que cette attaque n'aurait pas pu aboutir si au moins l'une des deux mesures détaillées ci-dessus avait été prise par la société.
Enfin, la société soulève que le principe de légalité des délits et des peines impose de définir dans des termes suffisamment clairs et précis les éléments constitutifs d'une infraction. Elle estime qu'en l'espèce, l'article 34 de la loi Informatique et Libertés est lacunaire s'agissant du type de mesures à prendre par le responsable de traitement.
La formation restreinte rappelle que le législateur a confié au responsable de traitement le choix des mesures précises à mettre en place pour respecter l'obligation générale tirée de l'article 34 précitée. En conséquence, le texte n'est pas prescriptif quant aux mesures à déployer pour garantir la sécurité d'un traitement, tant que l'obligation est, *in fine,* respectée.
Sur la base de ces éléments, la formation restreinte considère que le manquement à l'article 34 de la loi du 6 janvier 1978 modifié est constitué dès lors que la société n'a pas pris toutes les précautions utiles afin d'empêcher que des tiers non autorisés aient accès aux données traitées.

Sur la sanction et la publicité

Aux termes du I de l'article 45 de la loi du 6 janvier 1978 modifiée, dans sa version applicable au jour des constats *:*
Lorsque le responsable d'un traitement ne respecte pas les obligations découlant de la présente loi, le président de la Commission nationale de l'informatique et des libertés peut le mettre en demeure de faire cesser le manquement constaté dans un délai qu'il fixe. En cas d'extrême urgence, ce délai peut être ramené à vingt-quatre heures.

Si le responsable du traitement se conforme à la mise en demeure qui lui est adressée, le président de la commission prononce la clôture de la procédure. Dans le cas contraire, la formation restreinte de la commission peut prononcer, après une procédure contradictoire, les sanctions suivantes :
1° Un avertissement ;
2° Une sanction pécuniaire, dans les conditions prévues à l'article 47, à l'exception des cas où le traitement est mis en œuvre par l'Etat ;
3° Une injonction de cesser le traitement, lorsque celui-ci relève de l'article 22, ou un retrait de l'autorisation accordée en application de l'article 25.
Lorsque le manquement constaté ne peut faire l'objet d'une mise en conformité dans le cadre d'une mise en demeure, la formation restreinte peut prononcer, sans mise en demeure préalable, et après une procédure contradictoire, les sanctions prévues au présent I.
Les alinéas 1er et 2ème de l'article 47 de la loi précitée, dans sa version applicable au jour des constats, précisent que :

Le montant de la sanction pécuniaire prévue au I de l'article 45 est proportionné à la gravité du manquement commis et aux avantages tirés de ce manquement. La formation restreinte de la Commission nationale de l'informatique et des libertés prend notamment en compte le caractère intentionnel ou de négligence du manquement, les mesures prises par le responsable du traitement pour atténuer les dommages subis par les personnes concernées, le degré de coopération avec la commission afin de remédier au manquement et d'atténuer ses effets négatifs éventuels, les catégories de données à caractère personnel concernées et la manière dont le manquement a été porté à la connaissance de la commission.
Le montant de la sanction ne peut excéder 3 millions d'euros .
La société estime qu'au regard des critères fixés par l'article 47 de la loi du 6 janvier 1978 modifiée, le montant de 100.000 euros proposé par le rapporteur est disproportionné.
Elle rappelle que l'attaque dont elle a été victime n'est pas le résultat d'une négligence de sa part, qu'elle a immédiatement pris des mesures afin d'en atténuer les effets négatifs, qu'elle a pleinement coopéré avec les services de la CNIL et que les seules données à caractère personnel concernées sont des adresses de courriers électroniques dont une partie n'est pas identifiante car non associées à des personnes physiques mais à des comptes test ou à des noms de sociétés partenaires. Elle rappelle également qu'elle n'a tiré aucun avantage du manquement et qu'elle n'a reçu aucune plainte de la part de ses utilisateurs.
La formation restreinte note que par certains aspects, l'attaque subie par la société peut être qualifiée de sophistiquée. Elle note par ailleurs que le nombre réduit de catégories de données extraites, en l'occurrence, des adresses de messagerie électronique et des mots de passe chiffrés, est de nature à diminuer le risque d'atteinte à la vie privée des personnes concernées. En outre, elle relève que la société a fait preuve de coopération avec les services de la CNIL.
Toutefois, la formation restreinte considère que la société a fait preuve de négligence en ce que certaines mesures élémentaires de sécurité n'ont pas été prises, permettant ainsi le succès de l'attaque. Par ailleurs, nonobstant les catégories de données concernées, la formation restreinte relève que la société n'apporte aucun élément permettant de minimiser significativement le nombre de 82,5 millions d'adresses électroniques. Elle estime donc que le volume de données impactées par la violation est considérable.
Au regard des éléments développés ci-dessus, les faits constatés et le manquement constitué à l'article 34 de la loi du 6 janvier 1978 modifiée justifient que soit prononcée une sanction d'un montant de 50.000 (cinquante mille) euros.
Enfin, la formation restreinte considère qu'au regard du nombre très important de données en cause, du contexte actuel dans lequel se multiplient les incidents de sécurité et de la nécessité de sensibiliser les internautes quant aux risques pesant sur la sécurité de leurs données, il y a lieu de rendre publique sa décision.

PAR CES MOTIFS

La formation restreinte de la CNIL, après en avoir délibéré, décide :

- **de prononcer à l'encontre de la société DAILYMOTION une sanction pécuniaire d'un montant de cinquante mille (50.000) euros ;**
- **de rendre publique sa délibération, qui sera anonymisée à l'expiration d'un délai de deux ans à compter de sa publication.**

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.