COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES

Délibération n°2016-315 du 13 octobre 2016

Délibération de la formation restreinte n° 2016-315 du 13 octobre 2016 prononçant un avertissement à l'encontre du PARTI SOCIALISTE

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, M. Philippe GOSSELIN et Mme Marie-Hélène MITJVAVILLE, 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° 2016-147C du 27 mai 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 une mission de vérification de tous traitements relatifs au site PARTI-SOCIALISTE.FR ;

Vu la décision de la Présidente de la Commission portant désignation d'un rapporteur, en date du 23 juin 2016 ;

Vu les procès-verbaux de constatations en ligne n° 2016-147/1 du 27 mai 2016 et de contrôle sur place n° 2016-147/2 du 15 juin 2016 ;

Vu le rapport de M. Philippe LEMOINE, commissaire rapporteur, notifié au Parti Socialiste par huissier le 8 juillet 2016 ;

Vu les observations écrites versées par le Parti Socialiste le 2 septembre 2016, ainsi que les observations orales formulées lors de la séance de la formation restreinte ;

Vu la demande de huis clos reçue le 2 septembre 2016 à laquelle il a été fait droit par lettre du 6 septembre 2016 ;

Vu les autres pièces du dossier ;

Etaient présents, lors de la séance de la formation restreinte du 13 septembre 2016 :

- M. Philippe LEMOINE, Commissaire, en son rapport ;

- Mme Catherine POZZO DI BORGO, Commissaire du Gouvernement adjoint, n'ayant pas formulé d'observations ;

- M. X du Parti Socialiste ;

- Maître Y, Avocat ;

Les représentants du Parti Socialiste ayant pris la parole en dernier ;

A adopté la décision suivante :

I. Faits et procédure

Le Parti Socialiste (ci-après le PS) est l'un des principaux partis politiques français. Il comptait, au 30 avril 2016, 111 450 adhérents.

Le 26 mai 2016, la Commission nationale de l'informatique et des libertés (ci-après CNIL ou la Commission) a été informée par l'éditeur du site zataz.com de l'existence d'une faille de sécurité entraînant une fuite de données à partir de l'URL https://archives.parti-socialiste.fr/adhesions/suivi/list_adhesion.php?hash=c93b6da517f84a37e1a7f92899fdabe6 .

Le 27 mai 2016, en application de la décision n° 2016-147C de la Présidente de la Commission, une délégation de la CNIL a effectué des vérifications en ligne qui ont permis de constater qu'il était possible d'accéder librement, à partir de l'URL précitée, à un répertoire du nom de domaine parti-socialiste.fr contenant plusieurs fichiers classés sous un onglet Adhésion , lui-même divisé en plusieurs sous-onglets intitulés en attente de traitement , Adhésion Non finalisé[e] et Adhésion Transmise .

La délégation a constaté qu'il était possible d'exporter, au format CSV, les données comprises dans ces pages et notamment les nom, prénom, adresses électronique et postale des personnes.

La délégation a, par ailleurs, constaté que le sous-onglet Adhésion Transmise donnait accès au contenu de plusieurs dossiers nominatifs contenant tout ou partie des données suivantes : nom, prénom, adresses postale et électronique, numéros de téléphone fixe et mobile, date de naissance, adresse IP, moyen de paiement et montant de la cotisation.

En outre, la délégation a constaté qu'il était possible d'accéder, à partir de l'onglet paramètres à la Liste des utilisateurs de la plateforme, qui répertorie notamment les adresses électroniques et login de douze personnes. Par ailleurs, en cliquant sur le bouton ajouter un utilisateur , la délégation a constaté l'affichage d'une page intitulée Ajout d'un utilisateur permettant de renseigner les champs suivants : nom de la personne, prénom, identifiant, mot de passe, adresse électronique et service de l'utilisateur.

La Commission a alerté le jour même, par téléphone, le PS de l'existence de cette fuite de données. Celui-ci a indiqué prendre immédiatement les mesures correctives nécessaires pour la faire cesser.

Lors d'une seconde mission de contrôle effectuée le 15 juin 2016 dans les locaux du PS, la délégation a été informée par le directeur des systèmes d'information que le répertoire librement accessible à l'URL précitée correspond à la plateforme de suivi des paiements des primo-adhésions effectués en ligne depuis le site internet du PS. Il lui a été précisé que toutes les vingt-quatre heures, un flux informatique transmet la liste des inscriptions validées par le service administratif à la base de données des adhérents au PS ROSAM .

La délégation a, par ailleurs, constaté la présence de 98 999 enregistrements dans la base de données de suivi des primo-adhésions en ligne dont 71 467 enregistrements notés comme transmis à la base de données ROSAM . Il lui a, en effet, été précisé que certains de ces

enregistrements se rapportent à des inscriptions fantaisistes ou sont signalés comme des fraudes par le logiciel de paiement en ligne.

Le PS a, par ailleurs, indiqué qu'aucune durée de conservation des données contenues dans la plateforme n'a été définie. Il a ainsi été constaté que cette dernière contient des demandes d'adhésion effectuées depuis 2010.

Concernant l'origine de la faille de sécurité, il a été indiqué à la délégation de contrôle que le hash présent dans l'URL permettant d'accéder aux données des adhérents correspondait à un ensemble hashé en MD5 sans sel des nom, prénom et mot de passe lui-même hashé en MD5 sans sel . Ainsi, selon le directeur des systèmes d'information, cette URL a été obtenue par l'injection d'un script javascript dans un formulaire d'adhésion car une fiche adhérent dont les champs nom et prénom contiennent du code javascript a été identifiée. Ceci a été constaté par la délégation. Il lui a été précisé que ces formulaires avaient été corrigés et que ce type d'injection n'était plus faisable.

La délégation a, par ailleurs, été informée qu'après l'appel téléphonique de la CNIL du 27 mai 2016 pour signaler la faille, plusieurs mesures correctives avaient été mises en œuvre par le PS : blocage temporaire du site au moyen d'un htaccess , suppression du compte de la personne à partir de laquelle les données étaient accessibles, modification du nom du répertoire et réinitialisation de l'ensemble des mots de passe. La délégation de contrôle a toutefois constaté que seul le directeur des systèmes d'information avait changé son mot de passe, les utilisateurs de la plateforme de suivi des paiements ne pouvant le changer eux-mêmes.

Il lui a également été indiqué que, dans un second temps, la procédure d'authentification des personnes au site avait été modifiée pour créer deux niveaux de protection et qu'un système de traçabilité était en cours de développement.

Ces mesures ont été précisées dans un courrier adressé à la Présidente de la CNIL le 16 juin 2016. Le système d'authentification au site est ainsi passé de la méthode GET à la méthode POST et un token d'authentification a été défini, avec une limitation temporelle, afin de remplacer le secret passé en paramètre de l'URL. Enfin, le protocole sécurisé https a été déployé sur l'ensemble du site.

Aux fins d'instruction de ces éléments, la Présidente de la Commission a désigné M. Philippe LEMOINE en qualité de rapporteur, le 23 juin 2016, sur le fondement de l'article 46 de la loi du 6 janvier 1978 modifiée.

A l'issue de son instruction, le rapporteur a notifié au PS, par porteur, le 8 juillet 2016, un rapport détaillant les manquements à la loi qu'il estimait constitués en l'espèce. Ce rapport proposait à la formation restreinte de la Commission de prononcer un avertissement, dont il sollicitait par ailleurs qu'il soit rendu public.

Etait également jointe au rapport une convocation à la séance de la formation restreinte du 13 septembre 2016 indiquant au PS qu'il disposait d'un délai d'un mois pour communiquer ses observations écrites, ce délai étant repoussé en raison de la période estivale à la date du 5 septembre 2016.

Le PS a produit le 2 septembre 2016 des observations écrites sur le rapport, réitérées oralement lors de la séance de la formation restreinte tenue à huis-clos le 13 septembre 2016.

II. Motifs de la décision

1. 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 .

Il appartient à la formation restreinte de décider si le PS a manqué à l'obligation lui incombant 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 relatives aux personnes enregistrées dans la plateforme de suivi des paiements des primo-adhésions, notamment afin que ces données ne soient pas accessibles à des tiers non autorisés.

En défense, le PS reconnaît l'existence de la fuite de données constatée mais souligne sa bonne foi en rappelant que la faille de sécurité est survenue à son insu lors de la modification de l'application de suivi des paiements des primo-adhésions intervenue le 12 mai 2016.

Il affirme, par ailleurs, que la faille de sécurité n'a pas eu de conséquences dommageables dès lors que celle-ci a été brève, qu'il n'est pas établi que des internautes aient eu accès auxdites données et que ces dernières étaient d'une portée limitée . Le PS soutient ainsi que la donnée la plus sensible était celle faisant état d'une adhésion à un parti politique qui est, de son point de vue, un acte militant et public que leurs auteurs ne cherchent généralement pas à dissimuler.

Le PS insiste également sur sa particulière réactivité qui l'a conduit à prendre des mesures correctives immédiatement après le signalement de la CNIL et, ce, sans attendre une mise en demeure de la Commission.

La formation restreinte considère que la circonstance selon laquelle l'origine de la faille est involontaire n'est pas de nature à amoindrir la gravité du manquement et de ses effets, et ne saurait en aucune façon exonérer l'organisme de sa responsabilité.

Elle rappelle à ce titre la particulière ampleur de l'incident qui a concerné 71 467 primo-adhérents.

Elle relève par ailleurs que la gravité de la faille est accentuée par la nature et le nombre d'informations concernées et rappelle que cette fuite a bien permis la divulgation de données sensibles au sens de l'article 8 de la loi du 6 janvier 1978 modifiée. Les données en cause permettaient en effet de faire apparaître directement les opinions politiques des personnes concernées, notamment parce qu'il était possible de déterminer celles qui avaient été intégrées à la base de données des adhérents du PS. Elle rappelle qu'il s'agit d'informations relevant de la vie privée des personnes que ces dernières doivent être libres de révéler ou non et qui, en leur qualité de données sensibles , auraient dû faire l'objet de garanties de sécurité particulières.

La formation restreinte, tout en soulignant la bonne foi du PS qui a réagi immédiatement après la révélation de la faille pour corriger cette dernière, relève toutefois que les mesures élémentaires de sécurité n'avaient pas été prises en amont.

La formation restreinte considère, tout d'abord, que l'utilisation de la méthode dite GET , qui intègre le secret d'authentification de l'utilisateur dans les paramètres de l'URL, constitue une défaillance importante en termes de sécurité et de confidentialité. Il s'agit, en effet, d'une méthode considérée comme non fiable au regard des règles de l'art dès lors qu'elle permet à tout utilisateur ayant connaissance de l'URL de récupérer les informations relatives à l'authentification et de les exploiter. A cet égard, la formation restreinte note que le PS a, par la suite, utilisé un système d'authentification sécurisé, tel que la méthode dite POST , afin de rendre inexploitables les données obtenues et d'empêcher l'accès à l'interface d'administration de sa base de données.

La formation restreinte relève de surcroît que le secret contenu au sein de l'URL était transformé à l'aide de l'algorithme de hachage MD5 sans sel, méthode obsolète qui ne permet pas d'assurer la sécurité des données. Il est ainsi rappelé que pour empêcher toute attaque dite par force brute , une fonction de hachage doit non seulement être réputée forte mais également faire intervenir un aléa dans son calcul par l'injection d'un sel.

Enfin, la formation restreinte estime que le contrôle de la CNIL a permis d'établir que le PS n'avait pas mis en œuvre de système de traçabilité des connexions à la plateforme de suivi des paiements des primo-adhésions. La mise en place d'un tel dispositif constitue pourtant une précaution d'usage essentielle dont la mise en œuvre aurait permis, d'une part, d'identifier l'éventuelle exploitation malveillante de la faille de sécurité de la base de données et, d'autre part, d'intervenir immédiatement pour la corriger.

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.

2. Sur le manquement à l'obligation de définir et mettre en œuvre une durée de conservation des données

L'article 6-5° de la loi du 6 janvier 1978 modifiée prévoit que les données à caractère personnel sont conservées pendant une durée qui n'excède pas [celle] nécessaire aux finalités pour lesquelles elles sont collectées et traitées .

Lors du contrôle sur place effectué le 15 juin 2016, le PS a indiqué qu'aucune durée de conservation n'avait été définie pour les données contenues dans la plateforme de suivi des paiements des primo-adhésions. La délégation a par ailleurs constaté que la base contient des demandes d'adhésion effectuées depuis 2010.

En défense, le PS indique qu'en vertu de ses statuts, la cotisation due au titre d'une première adhésion est d'un montant modeste alors que le renouvellement est ensuite fixé sur la base d'un barème progressif prenant en compte les capacités contributives des adhérents. Il explique ainsi que la plateforme de suivi des primo-adhésions lui permet à la fois d'être informé des nouvelles adhésions et de l'effectivité du paiement des cotisations mais également de déterminer le montant de ces dernières en vérifiant si une demande constitue bien une primo-adhésion et non un renouvellement.

Le PS souligne, en conséquence, que les données de la plateforme ne peuvent être limitées dans le temps, une longue période pouvant s'écouler entre une primo-adhésion et un renouvellement.

La formation restreinte rappelle que les termes mêmes de l'article 6-5 précité interdisent la conservation sans limitation de durée de données à caractère personnel. Le Conseil d'Etat a d'ailleurs rappelé dans une décision du 18 novembre 2015 qu'une durée illimitée de conservation des données ne pouvait être regardée comme nécessaire aux finalités d'un traitement (CE, 18 novembre 2015, n° 372111).

Par ailleurs, la formation restreinte considère qu'en l'espèce, la nécessité d'identifier les primo-adhésions ne permet pas de justifier de l'intérêt à conserver en base active les données à caractère personnel des primo-adhérents pour une durée illimitée. Elle rappelle que la fixation d'une durée de conservation n'impose pas nécessairement la destruction des données à caractère personnel après l'expiration d'un certain délai mais, à tout le moins, leur versement en archives intermédiaires qui permet leur consultation uniquement par un nombre restreint de personnes habilitées.

A cet égard, la formation restreinte considère que le respect de cette obligation aurait permis de limiter l'ampleur de la faille de sécurité puisque seules les données les plus récentes et non celles collectés depuis 2010 auraient été rendues librement accessibles.

Le manquement aux obligations découlant de l'article 6-5° de la loi du 6 janvier 1978 modifiée est, dès lors, caractérisé.

III. Sur la sanction et la publicité

Les manquements commis par le PS justifient que soit prononcé à son encontre un avertissement.

Compte tenu de la gravité des manquements constatés, du nombre de personnes concernées par la faille et du caractère particulièrement sensible des données en cause, la formation restreinte décide de rendre publique sa décision.

PAR CES MOTIFS

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

- de prononcer un avertissement à l'encontre du Parti Socialiste ;

- 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