Commission Nationale de l'Informatique et des Libertés

Délibération n°SAN-2018-012 du 26 décembre 2018
Délibération de la formation restreinte n°SAN-2018-012 du 26 décembre 2018 prononçant une sanction pécuniaire à l'encontre de la société BOUYGUES TELECOM

La Commission nationale de l'informatique et des libertés, réunie en sa formation restreinte composée de M. Jean-François CARREZ , président, M. Alexandre LINDEN, vice-président, Mme Dominique CASTERA, Mme Marie-Hélène MITJAVILE et Monsieur Maurice RONAI, membres ;

Vu la Convention no 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 directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

Vu la loi no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée, notamment ses articles 45 et suivants ;

Vu le décret no 2005-1309 du 20 octobre 2005 pris pour l'application de la loi no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifié par le décret no 2007-451 du 25 mars 2007 ;

Vu la délibération no 2013-175 du 4 juillet 2013 portant adoption du règlement intérieur de la Commission nationale de l'informatique et des libertés ;

Vu la décision no 2018-058C du 6 mars 2018 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 de l'ensemble des traitements de données à caractère personnel accessibles ou ayant été accessibles depuis le domaine bouyguestelecom.fr ;

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 1er octobre 2018 ;

Vu le rapport de M. François PELLEGRINI, commissaire rapporteur, notifié à la société BOUYGUES TELECOM le 5 octobre 2018 ;

Vu les observations écrites du conseil de la société BOUYGUES TELECOM reçues le 31 octobre 2018 ;

Vu la réponse du rapporteur aux observations de la société BOUYGUES TELECOM, notifiée le 15 novembre 2018 au conseil de la société ;

Vu les nouvelles observations écrites du conseil de la société BOUYGUES TELECOM reçues le 29 novembre 2018 ainsi que les observations orales formulées lors de la séance de la formation restreinte ;

Vu les autres pièces du dossier ;

Étaient présents, lors de la séance de la formation restreinte du 13 décembre 2018 :

M. François PELLEGRINI, commissaire, en son rapport ;

En qualité de représentant de la société BOUYGUES TELECOM :

Les représentants de la société BOUYGUES TELECOM ayant pris la parole en dernier ;

A adopté la décision suivante :

I- Faits et procédure

La société BOUYGUES TELECOM est un opérateur de télécommunications français sis 37-39 rue Boissière à Paris (75116). Le capital de la société est détenu à 90,5 % par le groupe Bouygues et à 9,5 % par le groupe JCDecaux.

L'entreprise compte environ 7 000 salariés et 17,8 millions de clients (14,4 millions de clients pour la téléphonie mobile et 3,4 millions de clients box). Elle a réalisé, en 2017, un chiffre d'affaires de plus de 5 milliards d'euros, pour un résultat net de 260 millions d'euros.

Dans le cadre de son activité commerciale, elle édite et gère le site web www.bouyguestelecom.fr et offre à ses clients, sur cette plateforme, la possibilité de se connecter à un espace personnel afin, notamment, d'éditer des documents administratifs liés à leur contrat, dont des factures.

Le 2 mars 2018, la Commission nationale de l'informatique et des libertés (ci-après la CNIL ou la commission) a été informée, dans le cadre d'un signalement, de l'existence d'un défaut de sécurité sur le site web www.bouyguestelecom.fr. Ce courriel faisait état de la possibilité d'accéder à des documents contenant des données à caractère personnel de clients de la société à partir de plusieurs adresses URL ayant une structure identique.

Les 6 mars 2018, la société BOUYGUES TELECOM a notifié à la CNIL la violation de données par le biais du formulaire mis à disposition par la commission.

Le 9 mars 2018, en application de la décision no 2018-058C du 6 mars 2018 de la présidente de la commission, une délégation de la CNIL a procédé à une mission de contrôle dans les locaux de la société BOUYGUES TELECOM. À l'occasion de ce contrôle, la délégation a été informée que la société avait été avisée de la violation de données par un message adressé à son compte institutionnel sur le réseau social Twitter.

A la suite du signalement, les équipes de la société ont reproduit l'incident : les adresses URL composées comme suit https://www.bouyguestelecom.fr/archived/index/printcontract/archived_id/X, où X représente un nombre entier, permettaient d'afficher le contrat de souscription d'un client. À partir de cette adresse URL, et en modifiant la valeur de X , il était possible d'afficher le contrat d'un

autre client.

Les données concernées par la violation étaient contenues dans une table, intitulée archived_contract_invoice , composant la base de données MySQL du site de la société. Parmi les 2 788 289 lignes de la table, la société a indiqué que la violation ne permettait d'accéder qu'aux données contenues dans 2 176 236 lignes visant des clients B&You, sans comprendre de clients Bouygues Telecom ni de clients professionnels.

Une première série de mesures a été déployée le 5 mars 2018 afin d'empêcher l'accès aux données, avant que les équipes techniques ne découvrent l'origine exacte de la vulnérabilité et y remédient.

Lors du contrôle sur place du 9 mars 2018, la délégation a constaté qu'il n'était effectivement plus possible d'afficher les contrats et factures accessibles à partir des URL susvisées. Le contrôle a permis de constater que la saisie de plusieurs adresses URL composées comme suit https://www.bouyguestelecom.fr/archived/index/printcontract/archived_id/X renvoyait un message d'erreur que l'on soit, ou non, un utilisateur connecté à son espace client. Les données avaient donc effectivement été rendues inaccessibles.

Interrogée sur la date à laquelle le défaut de sécurité était apparu, la société a expliqué que la vulnérabilité trouvait son origine dans la fusion des marques Bouygues Telecom et B&You et des systèmes informatiques correspondants, en 2015. Une base spécifique aux anciens clients B&You a été conservée par la société afin de permettre à ces clients et anciens clients d'accéder à leurs contrats et factures. Il s'agit de la base de données concernée par la violation de données.

À l'occasion de tests effectués à la suite de la fusion de ces bases de données, le code informatique rendant nécessaire l'authentification au site web www.bouyguestelecom.fr avait été désactivé. En raison d'une erreur humaine commise par une personne agissant pour le compte de la société, ce code n'a pas été réactivé à l'issue des tests réalisés.

Aux fins d'instruction de ces éléments, la présidente de la commission a désigné M. François PELLEGRINI en qualité de rapporteur, le 1er octobre 2018, sur le fondement de l'article 46 de la loi du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés (ci-après loi du 6 janvier 1978 modifiée ou loi Informatique et Libertés).

À l'issue de son instruction, le rapporteur a notifié à la société BOUYGUES TELECOM le 5 octobre 2018 un rapport détaillant les manquements à la loi qu'il estimait constitués en l'espèce et a proposé à la formation restreinte de la CNIL 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 13 décembre 2018 et invitait la société à produire des observations en réponse dans un délai d'un mois.

Le 31 octobre 2018, la société a, par l'intermédiaire de son conseil, produit des observations écrites auxquelles le rapporteur a répondu le 15 novembre suivant en application des dispositions prévues par l'article 75 du décret no 2005-1309 du 20 octobre 2005 modifié. Dans sa réponse, le rapporteur proposait de réduire la sanction prononcée à un montant de deux cent cinquante mille (250 000) euros.

Le 29 novembre 2018, par l'intermédiaire de son conseil, la société a produit de nouvelles

observations en réponse à celles du rapporteur.

Elle a réitéré oralement l'ensemble de ses observations devant la formation restreinte le 13 décembre 2018.

II- 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, dans sa version applicable au jour des constats, 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 .

À 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 la violation de 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 erreur humaine. 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 dans lesquelles serait intervenue cette violation, et fait peser sur lui une obligation de résultat en matière de sécurité.

La formation restreinte rappelle qu'en application de l'article 34 précité, il appartient bien à la formation restreinte de décider si la société BOUYGUES TELECOM a manqué à l'obligation lui incombant de prendre des mesures suffisantes pour assurer la sécurité des données personnelles contenues dans son système d'information, et en particulier celles des utilisateurs du site web www.bouyguestelecom.fr. La formation restreinte relève à cet égard que la société BOUYGUES TELECOM ne conteste ni le fait que des données à caractère personnel qu'elle traite ont été librement accessibles par le biais des adresses URL évoquées, ni l'origine de cette violation de données.

En premier lieu, sur la mesure de protection mise en place, la société considère qu'elle a respecté les règles de l'art en mettant en place, au moment de la fusion de ses systèmes d'information, un mécanisme rendant nécessaire l'authentification de l'utilisateur avant de lui permettre d'accéder aux données sur le site web www.bouyguestelecom.fr. Elle considère qu'une seconde mesure de protection, telle que le fait de rendre les adresses URL imprévisibles ou difficilement lisibles, n'est une pratique imposée ni par les textes, ni par l'état de l'art.

Sur ce point, la formation restreinte constate que l'article 34 précité n'est pas prescriptif quant aux mesures devant être déployées par les responsables de traitement pour garantir la sécurité d'un traitement tant que l'obligation est, in fine, respectée.

La formation restreinte considère ainsi que bien qu'une mesure visant à rendre les adresses URL imprévisibles puisse apparaitre adaptée et proportionnée en l'espèce, au regard du nombre de données à caractère personnel accessibles, de la nécessité de les protéger, et de la fragilité induite par l'existence d'adresses URL prévisibles, cette mesure ne présente

effectivement pas un caractère obligatoire, d'autres mesures pouvant permettre d'assurer une protection équivalente des données traitées. Les précautions à prendre pour préserver la sécurité des données relèvent de la responsabilité du responsable de traitement.

La formation restreinte constate qu'en l'espèce, la société BOUYGUES TELECOM a fait le choix de ne pas mettre en œuvre de mesure complémentaire à l'authentification des utilisateurs du site web www.bouyguestelecom.fr. En conséquence, la formation restreinte estime que ce choix a fait peser sur la société une obligation particulièrement renforcée quant à la vigilance qu'il convenait de porter à cette unique mesure de sécurité.

En second lieu, sur l'attention portée à la mesure de protection mise en place, la société affirme avoir réalisé de nombreux audits et tests de sécurité afin de mettre à l'épreuve la protection des données à caractère personnel qu'elle traite. Ces tests ont été réalisés chaque année, tant directement par la société que par l'intermédiaire de prestataires extérieurs, entre 2015 et 2018. Elle rappelle qu'aucun de ces tests n'a permis de découvrir la vulnérabilité rendant accessibles les données.

La société explique l'absence d'efficacité de ces tests en raison de la méthode retenue : elle indique que des comptes d'utilisateurs factices sont créés à l'occasion de ces tests afin de simuler les actions réalisables par un utilisateur réel, et que ces comptes doivent être régulièrement générés pour adapter les tests à l'évolution de l'environnement informatique. Les comptes utilisés pour les tests effectués se sont donc révélés non adaptés pour identifier la vulnérabilité puisque seuls des comptes de clients B&You créés entre juillet 2011 et décembre 2014 pouvaient révéler la vulnérabilité ici en cause.

La société affirme également qu'il lui était matériellement impossible d'effectuer efficacement une revue manuelle des […] lignes qui composaient le code informatique de son site web.

Si la formation restreinte constate que la société justifie de la réalisation de plusieurs tests d'intrusion et de plusieurs audits portant sur le code de son site web, elle relève que ces tests n'étaient pas adaptés aux spécificités de la base héritée et qu'ils ne pouvaient amener à la découverte de la vulnérabilité. Ces tests étaient donc inefficaces en l'espèce.

De la même manière, si la formation restreinte pourrait admettre qu'une revue manuelle de l'ensemble du code du site web de la société peut ne pas être proportionnée au regard du nombre de lignes composant ce code, la formation restreinte estime néanmoins que l'attention particulière à apporter au mécanisme d'authentification nécessitait une revue manuelle du code portant uniquement sur cet élément critique. Une telle mesure n'apparaît en effet pas disproportionnée dans ce cas précis, tant au regard des moyens humaines et techniques à disposition de la société BOUYGUES TELECOM que des risques encourus par plus de deux millions de personnes concernées par la violation.

La formation restreinte constate en outre que le code commenté comportait spécifiquement l'indication qu'il devait être supprimé à l'issue de la phase de test. Une revue manuelle de ces lignes aurait ainsi immédiatement permis la découverte de l'erreur à l'origine de la vulnérabilité.

La formation restreinte estime dès lors que, si l'oubli de réactiver le code rendant nécessaire l'authentification des utilisateurs sur le site web de la société est effectivement une erreur

humaine, dont la société ne peut se prémunir totalement, le fait de ne pas avoir mis en œuvre, pendant plus de deux années, les mesures efficaces permettant de découvrir cette erreur constitue une violation des obligations imposées par l'article 34 susvisé. Des mesures de revue automatisée du code adaptées aux spécificités du système d'information hérité et une revue manuelle de la partie du code en charge de l'authentification auraient permis de découvrir la vulnérabilité et d'y remédier.

La formation restreinte considère, par conséquent, que la société n'a pas porté à la base en question l'attention nécessaire pour assurer la sécurité des données personnelles 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'État ;
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 2e 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 considère que le montant de 250 000 euros proposé par le rapporteur n'est pas justifié dans la mesure où les données concernées par la violation ne sont pas des données

sensibles, qu'elle a réagi promptement en prenant les mesures nécessaires afin de limiter l'impact de la violation, que la violation n'a causé aucun préjudice aux personnes concernées et qu'elle a coopéré avec la CNIL.

La formation restreinte constate que la société BOUYGUES TELECOM a été très réactive dans la mise en place d'une cellule de crise et le déploiement de mesures visant à rendre inaccessibles les données à caractère personnel concernées. La rapidité de la correction est nécessairement prise en compte par la formation restreinte pour venir modérer le montant de la sanction, bien qu'au demeurant, elle démontre également la simplicité de la vulnérabilité à l'origine de la violation de données.

La formation restreinte constate également que la société a mis en œuvre un grand nombre de mesures afin de minimiser l'impact d'une éventuelle violation de données pour ses clients, notamment le rappel des bonnes pratiques et la mise à disposition de fiches contenant des conseils pour ses clients, la lutte contre le phishing, la surveillance du dark web et la formation de ses salariés.

Néanmoins, la formation restreinte considère que la gravité de la violation est caractérisée en raison du nombre de données et de personnes concernées par la violation ainsi qu'en raison de sa durée.

Elle souligne en effet que la violation de données a concerné plus de deux millions d'utilisateurs, soit un nombre très important de personnes, et des données identifiantes telles que le nom, le prénom, la date de naissance, l'adresse de courrier électronique, l'adresse physique, le numéro de téléphone mobile. Elle relève en outre que la durée pendant laquelle, faute de vigilance adaptée, les données ont été accessibles librement et sans contrôle a été particulièrement longue (plus de deux ans et trois mois).

Elle rappelle ensuite que le fait que les données accessibles ne contiennent aucune donnée pouvant être qualifiée de sensible , au sens de l'article 8 de la loi Informatique et Libertés , est sans influence sur la caractérisation du manquement à l'obligation incombant à un responsable de traitement d'assurer la sécurité des données qu'il traite.

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 250 000 (deux cent cinquante mille) euros.

Enfin, la formation restreinte considère qu'au regard de la gravité du manquement précité, du contexte actuel dans lequel se multiplient les incidents de sécurité et de la nécessité de sensibiliser les responsables de traitements et les internautes quant aux risques pesant sur la sécurité des données, il y a lieu de rendre publique sa décision, conformément à l'article 46 de la loi du 6 janvier 1978.

PAR CES MOTIFS

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

de prononcer à l'encontre de la société BOUYGUES TELECOM une sanction pécuniaire d'un montant de 250 000 (deux cent cinquante mille) euros ;
de rendre publique sa délibération sur le site de la CNIL et sur le site Légifrance, 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’État dans un délai de deux mois à compter de sa notification.