Délibération n° 2021-256 du 17 novembre 2021

de la Commission de Contrôle des Informations Nominatives portant avis favorable à la mise en œuvre du traitement automatisé d'informations nominatives ayant pour finalité

« *Gestion des réseaux Wifi Guest* »

présenté par la Direction des Systèmes d'Information

représenté par le Ministre d'Etat

Vu la Constitution du 17 décembre 1962 ;

Vu la Convention Européenne de Sauvegarde des Droits de l'Homme et des Libertés Fondamentales du Conseil de l'Europe du 4 novembre 1950 ;

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 et son Protocole additionnel ;

Vu la Loi n° 1.165 du 23 décembre 1993 relative à la protection des informations nominatives, modifiée ;

Vu la Loi n° 1.430 du 13 juillet 2016 portant diverses mesures relatives à la préservation de la sécurité nationale ;

Vu la Loi n° 1.383 du 2 aout 2011 pour une Principauté numérique, modifiée ;

Vu l'Ordonnance Souveraine n° 2.230 du 19 juin 2009 fixant les modalités d'application de la Loi n° 1.165 du 23 décembre 1993, modifiée, susvisée ;

Vu l'Ordonnance Souveraine n° 7.996 du 12 mars 2020 portant création de la Direction des Systèmes d'Information ;

Vu la délibération n° 2011-82 du 21 octobre 2011 portant recommandation sur les principes européens applicables aux traitements automatisés ou non automatisés d'informations nominatives ;

Vu la demande d'avis déposée par le Ministre d'Etat, le 21 juillet 2021, concernant la mise en œuvre d'un traitement automatisé ayant pour finalité la « *Gestion des réseaux Wifi Guest* » ;

Vu la prorogation du délai d'examen de la présente demande d'avis notifiée au responsable de traitement le 17 septembre 2021, conformément à l'article 19 de l'Ordonnance Souveraine n° 2.230 du 19 juin 2009 susvisée ;

Vu le rapport de la Commission de Contrôle des Informations Nominatives en date du 17 novembre 2021 portant examen du traitement automatisé susvisé.

La Commission de Contrôle des Informations Nominatives,

Préambule

Afin de permettre la mise à disposition d'un accès Internet aux visiteurs des différents locaux du Gouvernement, sans impacter le Système d'Information de ce dernier, le Ministre d'Etat souhaite mettre en œuvre le traitement ayant pour finalité la « *Gestion des réseaux Wifi Guest* ».

Ainsi, ce dernier est soumis à l'avis de la Commission, conformément à l'article 7 de la Loi n° 1.165 du 23 décembre 1993.

I. Sur la finalité et les fonctionnalités du traitement

Le présent traitement a pour finalité « *Gestion des réseaux Wifi Guest* ».

Il concerne « *tout utilisateur du réseau Wifi Guest, ainsi que les fonctionnaires et agents de l'Etat pouvant valider la création d'un compte* ».

Les fonctionnalités du traitement sont :

- fournir un accès Wifi dédié aux personnels et prestataires du Gouvernement disposant ou non d'un compte AD (Wifi Guest Gouvernement) ;
- fournir un accès Wifi public (Wifi ServicePublic) ;
- permettre la connexion au WIFI Service Public par le biais des réseaux sociaux ;
- créer un compte/profil utilisateur ;
- identifier, authentifier et accéder au compte/profil ;
- conserver les données de trafic ou données de connexion dans le respect de la règlementation en vigueur ;
- les transmettre aux entités habilitées dans les hypothèses prévues par la règlementation en vigueur ;
- établissement de statistiques non nominatives.

La Commission constate que la finalité du traitement est déterminée et explicite, conformément aux dispositions de l'article 10-1 de la Loi n° 1.165 du 23 décembre 1993.

II. Sur la licéité et la justification du traitement

Le responsable de traitement indique que le présent traitement est justifié par le respect d'une obligation légale et la réalisation d'un intérêt légitime, sans que ne soient méconnus les droits et libertés fondamentaux des personnes concernées.

En ce qui concerne l'obligation légale, le responsable de traitement indique qu'il ressort des dispositions des articles 31, 32, 34 de la Loi n° 1.383 du 2 aout 2011 pour une Principauté numérique que *« les prestataires qui fournissent un accès au réseau de communication doivent détenir et conserver les données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elles sont*

prestataires ». La Commission constate que lesdites dispositions s'appliquent aux fournisseurs de services de communication au public en ligne, c'est-à-dire « *toute personne assurant la mise à disposition de contenus, services ou applications relevant de la communication au public en ligne, au sens de la présente loi. Sont notamment considérées comme des fournisseurs de services de communication au public en ligne les personnes qui éditent un service de communication au public en ligne, mentionnées à l'article 33 de la présente loi, ou celles qui assurent le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature mentionnées à l'article 29 de la présente loi* », ce qui n'est pas le cas du Gouvernement en l'espèce.

La Commission relève que le Gouvernement a introduit par Arrêté Ministériel n° 2017-579 du 19 juillet 2017 portant application de l'article 10 de la Loi n° 1.430 du 13 juillet 2016 portant diverses mesures relatives à la préservation de la sécurité nationale, quelles données de trafic peuvent être collectées par « *les personnes qui offrent un accès à des services de communications électroniques au public en ligne, y compris à titre gratuit* ». A cet égard, la collecte des URLs consultées et de mots clés tapés, dont le contenu relève de la vie privée des utilisateurs navigant sur le réseau Internet, n'est pas autorisée par les dispositions légales. Elle demande donc que les mots clés tapés par les visiteurs ne soient pas collectés.

Le responsable de traitement précise en outre que si deux réseaux « *guests* » coexistent, un dédié aux personnels et prestataires du Gouvernement, l'autre à des visiteurs externes sans lien avec l'Administration, tous deux doivent être considérés comme une offre d'accès à des services de communications électroniques au public en ligne. A cet égard, il indique que le réseau Wifi Guest Gouvernement n'est pas ouvert pour une utilisation à des fins professionnelles. La distinction entre les deux réseaux permet uniquement une offre de temps de connexion plus étendue aux personnels de l'Administration qu'aux simples visiteurs.

Il est enfin indiqué que ce traitement s'inscrit dans les missions définies à l'article 2 de l'Ordonnance Souveraine n° 7.996 du 12 mars 2020 portant création de la DSI, notamment en son point 2 qui dispose que la DSI est chargée « *d'assurer la gestion opérationnelle des infrastructures matérielles et logicielles constituant le système d'information de l'Administration en assurant une haute disponibilité des ressources informatiques* » et « *d'assurer la gestion des réseaux de téléphonie IP et wifi au sein de l'Administration* ».

Sous ces réserves, la Commission considère que ce traitement est licite et justifié, conformément aux dispositions des articles 10-1 et 10-2 de la Loi n° 1.165 du 23 décembre 1993.

III. Sur les informations traitées

Les informations nominatives traitées sont :

- identité : utilisateur : nom, prénom ; utilisateur authentifié par un réseau social : numéro (token), nom, prénom ;
- adresses et coordonnées : utilisateur : email ; agent de l'Administration « parrain pour le wifi Guest interne : email ;
- vie professionnelle : utilisateur pour le wifi guest interne : fonction, nom de l'entreprise ;
- données d'identification électronique : identifiant, mot de passe, token, login/mot de passe ;
- données de trafic : adresse MAC du terminal, identifiant de l'utilisateur, adresse mail, OS, type de navigateur, adresse IP de l'équipement utilisé, date, heure, durée de chaque connexion, information permettant d'identifier le destinataire de la communication (sans élément sur le contenu), action de filtrage et catégorie d'URL bloquée (le cas échéant) ;

- type d'accès : profil (prestataire/usager), type de service (full accès), zone d'entrée (interne/externe), plage horaire, durée de validité.

Les informations relatives à l'identité, aux adresses, à la vie professionnelle sont communiquées par l'utilisateur. Certaines informations peuvent provenir du réseau social choisi par l'utilisateur pour se connecter (nom, prénom, token).

Le login, les données de trafic et les informations sur les types d'accès sont produits par le système.

Par ailleurs, la Commission rappelle comme exposé au point II de la présente délibération, que l'Arrêté Ministériel n° 2017-579 du 19 juillet 2017 portant application de l'article 10 de la Loi n° 1.430 du 13 juillet 2016 portant diverses mesures relatives à la préservation de la sécurité nationale liste les données de trafic pouvant être collectées, ce qui ne comprend pas les URLs et les mots clés tapés par les utilisateurs du Wifi public, ce qui serait une atteinte disproportionnée à leur vie privée.

Enfin, il est constaté que des données liées à la journalisation des accès au présent traitement sont collectées.

Sous cette réserve, la Commission considère que les informations collectées sont « *adéquates, pertinentes et non excessives* » au regard de la finalité du traitement, conformément aux dispositions de l'article 10-1 de la Loi n° 1.165 du 23 décembre 1993.

IV. Sur les droits des personnes concernées

➢ *Sur l'information préalable des personnes concernées*

L'information préalable des personnes concernées est réalisée par le biais d'un document spécifique, à savoir la charte Wifi diffusée avant toute utilisation du réseau.

La Commission relève que la mention concernée, jointe au dossier, est conforme aux dispositions légales.

Elle relève toutefois qu'en cas d'accès au réseau WIFI par le biais de réseaux sociaux, certaines alertes formulées par la solution informent les personnes concernées de collectes de données les concernant qui sont larges et disproportionnées. Il appert cependant de l'analyse du dossier que seules les informations nécessaires à la connexion sont effectivement collectées. Elle en prend acte. Elle relève également les précisions du responsable de traitement qu'à défaut de pouvoir paramétrer lesdites alertes, des précisions pourraient être apportées dans la charte d'utilisation du service. La Commission recommande d'adopter cette solution.

➢ *Sur l'exercice du droit d'accès, de modification et de mise à jour*

Le droit d'accès est exercé par voie postale auprès de la Direction des Systèmes d'Information.

A cet égard, la Commission rappelle que la réponse à ce droit d'accès doit s'exercer dans le mois suivant la réception de la demande.

Elle constate que les modalités d'exercice des droits des personnes concernées sont conformes aux dispositions des articles 13, 15 et 16 la Loi n° 1.165, modifiée.

V. Sur les destinataires et les personnes ayant accès au traitement

Peuvent avoir communication des informations les « *tiers habilités, soit les autorités compétentes dans le cadre de leurs fonctions et des garanties prévues par les textes* ».

Le responsable de traitement indique qu'ont accès au traitement :

- le personnel habilité de la DSI dans le cade de ses fonctions, inscrit dans une chaine d'escalade (niveaux de droits différents) ;
- les prestataires, dans le cadre de leurs missions de maintenance.

A l'analyse du dossier il appert que l'équipe réseau de la DPRN a également accès au traitement ainsi que « *les administrateurs délégués* », « *les référents* » et les « *parrains* ».

En ce qui concerne le recours à des prestataires, elle rappelle que conformément aux dispositions de l'article 17 de la Loi n° 1.165 du 23 décembre 1993 le droit d'accès de ces derniers doit être limité à ce qui est strictement nécessaire à l'exécution de leurs contrats de prestation de service. De plus, lesdits prestataires sont soumis aux mêmes obligations de sécurité et de confidentialité que celles imposées au responsable de traitement, en application de ce même article.

La Commission considère que ces accès sont justifiés.

VI. Sur les rapprochements et les interconnexions avec d'autres traitements

Le responsable de traitement indique que le traitement est interconnecté avec les traitements légalement mis en œuvre suivants :

- « *Gestion centralisée des accès aux applications du SI* », afin de permettre l'authentification des accès des utilisateurs disposant d'un compte sur le réseau du Gouvernement ;
- « *Gestion et analyse des évènements du système d'information* » afin de veiller à la traçabilité et à la sécurité des accès au SI,
- « *Gestion des accès à distance au système d'information du Gouvernement* », aux fins de sécuriser les accès au SI ;
- « *Gestion de la messagerie professionnelle* », aux fins de recevoir les mails de demande d'accès et de valider ces demandes.

Il est également rapproché avec le traitement ayant pour finalité « *Assistance aux utilisateurs par le Centre de Service de la DSI* », légalement mis en œuvre.

La Commission constate que ces interconnexions et ce rapprochement sont conformes aux exigences légales et aux finalités initiales pour lesquelles les informations nominatives ont été collectées.

VII. Sur la sécurité du traitement et des informations

Les mesures prises pour assurer la sécurité et la confidentialité du traitement et des informations qu'il contient n'appellent pas d'observation.

Cependant les ports non utilisés doivent être désactivés et les serveurs, périphériques, équipements de raccordements (switchs, routeurs, pare-feux) ainsi que chaque compte utilisateur et administrateur doivent être protégés individuellement par un identifiant et par un mot de passe réputé fort, régulièrement renouvelé.

En outre, il appert de l'analyse du dossier que l'adresse MAC des équipements utilisés après une authentification au réseau Wifi est mémorisée (collectée) afin d'authentifier automatiquement l'utilisateur du wifi « *Wifi Guest Gouvernement* » à chaque future connexion. La commission relève notamment que si différents utilisateurs partagent des terminaux communs pour se connecter à leur profil et au WIFI, il apparait possible que la MAC adresse reconnue par le système soit nominativement associée à la personne ayant pour la première fois connecté le terminal au réseau WIFI, quelle que soit la personne qui se connecte ultérieurement audit réseau. Il peut donc y avoir un risque quant à une mauvaise imputabilité de responsabilité en cas d'utilisation non conforme du réseau WIFI.

La Commission demande donc au responsable de traitement de s'assurer que les données de trafic collectées soient bien attribuées à la personne qui utilise le réseau de manière effective en cas de ressources partagées.

La Commission rappelle enfin que, conformément à l'article 17 de la Loi n° 1.165 du 23 décembre 1993, les mesures techniques et organisationnelles mises en place afin d'assurer la sécurité et la confidentialité du traitement au regard des risques présentés par celui-ci et de la nature des données à protéger devront être maintenues et mises à jour en tenant compte de l'état de l'art, afin de permettre de conserver le haut niveau de fiabilité attendu tout au long de la période d'exploitation du présent traitement.

VIII. Sur la durée de conservation

Les données sont conservées un an glissant, excepté les données d'identification électronique qui sont conservées :

- tant que l'utilisateur a accès aux ressources du Gouvernement en ce qui concerne l'identifiant/mt de passe ;
- le temps de la durée de validité de l'accès en ce qui concerne le token ;
- 3 mois en ce qui concerne le login/mot de passe.

La Commission considère que ces durées sont conformes aux exigences légales.

Enfin, les données de journalisation visées au point III de la présente délibération ne pourront être conservées pour une durée qui ne peut être inférieure à 3 mois ni supérieure à un an à compter de leur collecte.

Après en avoir délibéré, la Commission :

Exclut la collecte de mots clés renseignés par les utilisateurs du présent traitement.

Demande au responsable de traitement de s'assurer que les données de trafic collectées sont bien attribuées à la personne qui utilise le réseau de manière effective en cas de ressources partagées.

Rappelle que :

- les fonctionnaires, agents de l'Etat et prestataires du réseau Wifi Guest Gouvernement doivent être informés des mesures de collecte/surveillance opérées lors de leur consultation de sites Internet ;

- les URLs consultées ne peuvent être collectées ;

- les ports non utilisés doivent être désactivés et les serveurs, périphériques, équipements de raccordements (switchs, routeurs, pare-feux) ainsi que chaque

compte utilisateur et administrateur doivent être protégés individuellement par un identifiant et par un mot de passe réputé fort, régulièrement renouvelé.

Fixe pour une durée qui ne peut être inférieure à 3 mois ni supérieure à un an à compter de leur collecte la conservation des données de journalisation.

Sous le bénéfice de la prise en compte de ce qui précède,

la Commission de Contrôle des Informations Nominatives **émet un avis favorable à la mise en œuvre, par le Ministre d'Etat, du traitement automatisé d'informations nominatives ayant pour finalité *« Gestion des réseaux Wifi Guest ».***

Le Président

Guy MAGNAN