Livre blanc

Almond

Léa Thomas, Consultante SSI experte en droit des nouvelles technologies

Adrien Gaillard, Senior consultant en sécurité des réseaux

Comment mettre en place un service de Wi-Fi public conforme au droit français ?

Focus sur les obligations techniques et juridiques

Almond | Janvier 2020

Sommaire

Introduction

La technologie de communication radio nommée Wi-Fi a commencé à être développée dans les années 1990. L'année 2002 marque un tournant dans l'expansion de cette technologie : l'Autorité de Régulation des Télécommunications (ART), ancêtre de l'ARCEP, a alors défini le cadre réglementaire pour l'établissement de réseaux Wi-Fi ouverts au public.

Le droit s'appliquant aux service Wi-Fi public répond à un certain nombre de problématiques et de risques. Au cours des 20 dernière années, le cadre règlementaire a fortement évolué au fil de l'accroissement des usages d'une part, mais aussi des risques et de la diversification de ces problématiques, dont la cybercriminalité. La cybercriminalité peut se caractériser par des infractions commisses contre un système d'information, utilisée afin de commettre des crimes et délits en tout genre (fraudes, visionnage de contenus illicites comme la pédopornographie, vol d'information d'authentification, etc.).

Ce document a ainsi pour objectif de répondre aux interrogations concernant plusieurs difficultés et contraintes rencontrés lorsqu'un service Wi-Fi public ou invité est présent au sein de l'entreprise, dont nous pouvons en citer quelques-unes :

- En premier lieu, les usages et les besoins des utilisateurs évoluent très rapidement. En effet, il est aujourd'hui considéré comme normal qu'un espace recevant du public propose un service Wi-Fi associé. De la même manière, il parait aller de soi qu'une entreprise recevant des partenaires, fournisseurs, clients propose un service Wi-Fi à ses invités, souvent nommé service « Guest » ;
- Comme dit plus haut, la règlementation évolue elle aussi et peut paraître complexe au regard des nombreux textes, des différentes jurisprudence, des apports par des textes récents comme le RGPD, etc. ;
- Certaines exigences peuvent aussi paraître contradictoire, particulière celles abordant le sujet de la protection des données à caractère personnel, et celles invoquant la traçabilité des données ;
- Les solutions techniques à mettre en œuvre sont parfois complexes et font appel à plusieurs domaines de compétences qui n'ont pas encore l'habitude de communiquer de manière fluide dans beaucoup d'entreprise (les compétences radio Wi-Fi, les compétences réseaux, les compétences sécurité) ;
- Et enfin, les menaces évoluent encore plus rapidement que la juridiction ou les aspects techniques, avec par exemple la généralisation du peer-to-peer, du piratage Wi-Fi, les accès au Darkweb, les attaques par déni de service, etc.

Aussi, ce document n'a pas pour objectif de mettre en garde sur les dangers de l'utilisation du Wi-Fi public mais bien de donner des pistes de réponses aux professionnels dans la mise en œuvre de ce type de service. Il présente notamment l'état actuel du droit et les bonnes pratiques pour la fourniture d'un service de Wi-Fi public.

1 Wi-Fi public, comment fonctionnent-ils ?

1.1 Les différents types de services Wi-Fi

Pour aller plus loin, nous avons besoin en premier lieu de définir les trois grandes familles de services Wi-Fi :

1. Le service Wi-Fi privé (ou Office) : ce type de service s'adresse à une population limitée et doit être soumis à des conditions d'utilisations définies dans une charte informatique. En outre, le service Wi-Fi privé se voit doté de fonction de contrôle et de sécurité en partie à la discrétion des administrateurs de la solution (l'entreprise dans le cas le plus courant) ;
2. Le service Wi-Fi invité (ou Guest) : ce type de service s'adresse à tout type d'invité qui n'aurait pas besoin d'accéder au SI privé de l'organisme, mais uniquement à Internet. Dans l'environnement de l'entreprise, la cible serait typiquement les fournisseurs, les clients, ou encore les partenaires de passage dans les locaux. De nombreuses entreprises autorisent aussi leurs collaborateurs à connecter leurs terminaux personnels à ce service Guest ;
3. Le service Wi-Fi public (ou Hotspot) : ce type de service s'adresse à tout type de population. La zone de fourniture de service est donc bien un espace public ou ouvert au public.

Ce document concerne non seulement les services Wi-Fi public, mais nous allons voir par la suite que les services Wi-Fi invité sont aussi sujets aux exigences juridiques liées aux services d'accès au réseau fournis au public.

1.2 Quelles données techniques sont échangées lors d'une connexion internet via un réseau Wi-Fi public ?

L'objectif est de comprendre quelles données sont échangées lors d'une connexion internet, via un réseau Wi-Fi public, afin de mettre en perspective les aspects techniques pour comprendre comment mettre en œuvre la collecte et le stockage d'informations à but légal. Ces informations ont pour objectif d'être utilisées à titre de preuve en cas de réquisition judiciaire.

Le schéma ci-dessous permet de comprendre l'enchainement des échanges qui se produisent lors de la première connexion d'un périphérique utilisateur à un service Wi-Fi muni d'une page de connexion, afin d'accéder à un site Internet. Il permet également d'identifier les informations techniques générées au cours de ces échanges (cf. indications en bleu dans le schéma).

Les données techniques décrites dans ce schéma sont celles devant être collectées dans le cadre de l'obligation de conservation prévue par le droit français dans le sens de notre interprétation et de notre expérience.

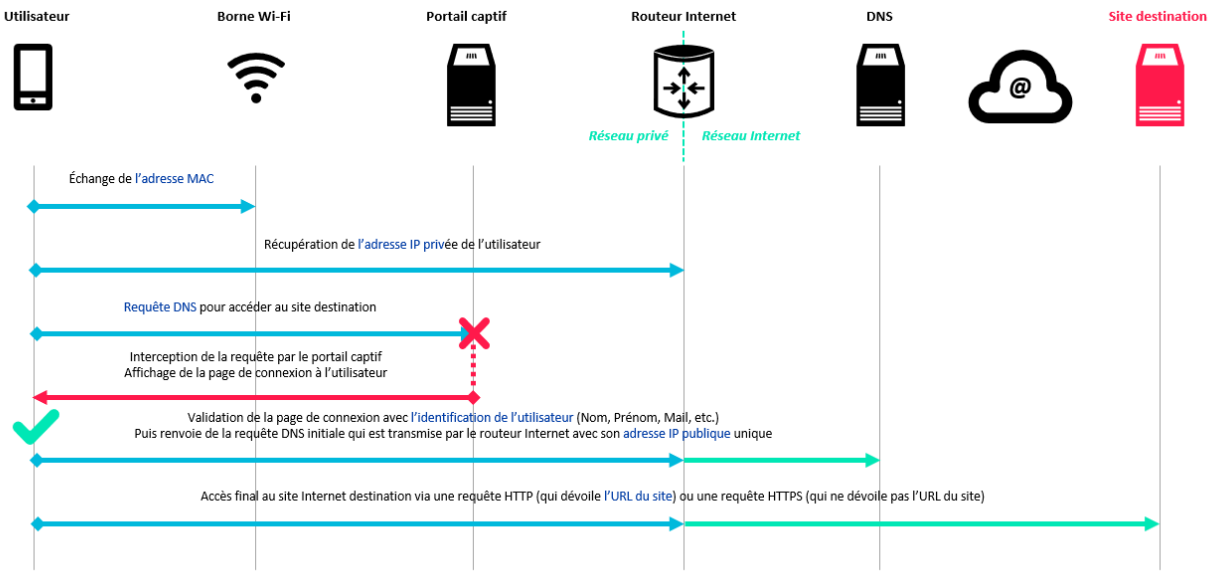

Schéma 1: Chronogramme simplifié des échanges en vue d'une connexion Internet sur un service Hotspot

Les éléments figurants dans la partie supérieure de ce schéma représentent les briques principales contactées. Ces briques permettent d'établir la communication finale avec le serveur web hébergeant le site de destination. La borne Wi-Fi permet à l'équipement utilisateur d'échanger avec l'infrastructure son ***adresse MAC*** en se connectant à un SSID (le réseau Wi-Fi Hotspot souhaité), pour permettre ensuite d'obtenir une ***adresse IP privée*** sur le réseau du fournisseur de service Hotspot auprès d'un routeur par exemple.

Une ***requête DNS*** est alors émise par l'équipement utilisateur pour tenter de résoudre le nom de domaine du site souhaité. Cette ***requête DNS*** est ensuite interceptée par le Portail Captif qui présente, en retour, la page obligatoire de connexion au service. C'est seulement via ***l'identification de l'utilisateur*** et/ou la validation des Condition Générales d'Utilisation (CGU) que le Portail Captif autorisera la connexion à s'orienter vers Internet, via l'utilisation de l'***adresse IP publique*** du fournisseur de service Hotspot.
Enfin, la résolution du nom de domaine auprès des services DNS du fournisseur d'accès (par exemple), permet de générer la première requête directe au site Internet, par l'émission d'une requête HTTP qui contient l'***URL du site destination***.

L'ensemble de ces informations peut être récupéré directement dans les communications, sans qu'il ne soit nécessaire d'analyser le contenu de ces communications : c'est l'analyse des métadonnées.

L'analyse du contenu des communications étant prohibé en droit français, il convient de savoir dissocier les données des métadonnées afin de comprendre quels éléments conserver.

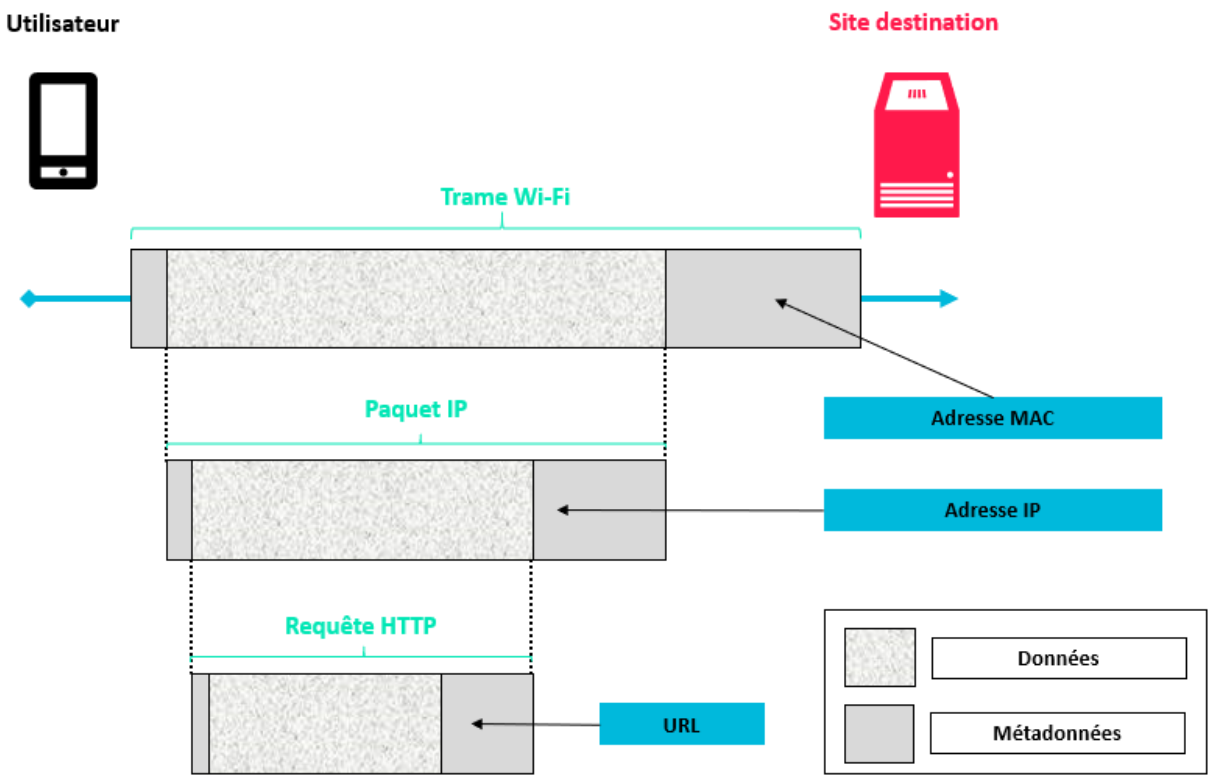

Schéma 2: Structure simplifiée des échanges de communication par paquet sur les réseaux TCP/IP

Le schéma ci-dessus permet de comprendre la structure des communications classiques sur nos réseaux pour dissocier données et métadonnées lors des différents types d'échanges vus précédemment.

Le contenu des pages web circule ainsi en tant que « corps » des paquets et trames sur le réseau, c'est à dire en tant que « Données ». Les entêtes qui contiennent les URL, les adresses IP, ou encore, les adresses MAC, permettent aux réseaux de transférer ces paquets de données de proche en proche et de traiter les mécanismes communicationnels sous-jacents.

Ces entêtes constituent les métadonnées qui correspondent aux informations essentielles, objets de l'obligation de conservation prévu par le Code des Poste et Communications Electroniques.

1.3 Quel est le statut juridique de ces données techniques ? La position des juridictions européennes et françaises concernant les adresses IP et MAC

Comme vu dans les schémas ci-dessus, les adresses IP et MAC représentent des métadonnées pouvant être collectées lors d'une connexion d'un utilisateur à internet via un réseau Wi-Fi.

Les tableaux ci-dessous présentent successivement des jurisprudences, des délibérations européennes et/ou françaises sur la qualification juridique des adresses IP et MAC.

ADRESSE MAC

	<u>Délibération CNIL, n°2011-035, 17 mars 2011</u> : La CNIL assimile l'adresse MAC à une donnée à caractère personnel si et seulement si, elle est combinée à d'autres données techniques telles que l'identifiant SSID ou des données de localisation.
Position de la CNIL	La formation restreinte de la CNIL a estimé : *« qu'une adresse MAC, qui n'identifie que le routeur Wi-Fi qui permet aux utilisateurs d'accéder à internet, ne peut être qualifiée, à elle seule, de donnée à caractère personnel. En revanche, une adresse MAC peut être captée par des sites Internet lors de la navigation de l'Internaute, après que ce dernier se soit identifié. Une fois reliée à ces éléments d'identification, elle constitue nécessairement une donnée personnelle. C'est en fonction de tels éléments de contexte qu'il convient de décider si une adresse MAC peut être considérée, ou non, comme une donnée à caractère personnel. »*
Position du Conseil d'Etat	**<u>Conseil d'Etat, 8 février 2017, n°393714 :</u>** Le Conseil d'Etat confirme la position de la CNIL en assimilant l'adresse MAC, des équipements terminaux des individus, à une donnée à caractère personnel lorsque celle-ci est couplée à des données de localisation.

ADRESSE IP

Position du G29	**<u>Avis du G29 du 20 juin 2007, WP 136</u> :** Le G29 relève que l'adresse IP attribuée à un internaute lors de ses communications constituait une donnée à caractère personnel
Position de la CJUE	**<u>CJUE, question préjudicielle, 19 octobre 2016, affaire C-582/14 :</u>** L'exploitant d'un site Internet peut avoir un intérêt légitime à conserver certaines données à caractère personnel des visiteurs de leur site afin de se défendre contre les attaques cybernétiques. La CJUE a l'occasion d'affirmer dans cet arrêt que l'IP dynamique d'un visiteur d'un site internet, constitue une donnée à caractère personnel lorsque l'exploitant du site internet dispose de moyens légaux lui permettant de faire identifier le visiteur. ⚠ Ce principe est valable même si l'exploitant du site internet ne dispose pas directement des moyens permettant d'identifier la personne.

Par ailleurs, s'agissant de données à caractère personnel, les organismes proposant au public, une connexion Wi-Fi, doivent se conformer au RGPD pour le traitement de ces données[1].

[1] Article L34-1 du CPCE, IV alinéa 3

2 L'encadrement législatif du Wi-Fi public pour la lutte contre la cybercriminalité

NB: Ce document s'appuie sur les lois et règlementations en vigueur au 31/01/2020. Un nouveau règlement européen (ePrivacy 2020) est en cours d'élaboration et devrait être finalisé prochainement avant son application aux législations nationales. Le présent document sera mis à jour en fonction des nouveaux contenus législatifs qui entreront en vigueur et qui s'appliqueront pour le domaine des services Wi-Fi.

2.1 Un équilibre nécessaire entre libertés des individus et lutte contre la cybercriminalité

La conservation des données issues de communications électroniques, bien que nécessaire pour la lutte contre la cybercriminalité, est selon le juge européen, une pratique devant être encadrée. En effet, les données conservées étant considérées comme des données à caractère personnel, d'importants gardes fous doivent être mis en place par les Etats-membres.

L'arrêt Digital Rights Ireland du 8 avril 2014 de la Cour de justice de l'Union européenne (CJUE) qui a invalidé la directive 2006/24/CE dite *« Data Retention »*, traite de la validité de mesures législatives prises afin de transposer en droit interne ladite directive. Dans cet arrêt la CJUE a eu l'occasion de se prononcer sur la conservation des données issues de communications électroniques.

Cette directive imposait aux opérateurs de communications électroniques, une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation. En effet, le juge européen a considéré qu'une conservation généralisée de ces données représentait une atteinte disproportionnée au droit fondamental du respect de la vie privée, duquel découle, la protection des données à caractère personnel.

En outre, la conservation des données relatives au trafic et des données de localisation peut présenter un risque pour les droits et libertés des personnes dans la mesure où, prises dans leur ensemble, les données conservées peuvent permettre de tirer des conclusions précises sur la vie privée des personnes : c'est ce qu'on appelle une inférence.

A ce titre, la CJUE rappelle que les dérogations à la protection des données à caractère personnel ne doivent intervenir que dans les limites du strict nécessaire.

Point d'attention : Les Etats membres ne peuvent pas imposer une obligation générale de conservation des données aux fournisseurs de services de communications électroniques.

Par ailleurs, le droit de l'UE ne s'oppose pas à ce que les Etats membres, prévoient, à titre préventif, une conservation des données relatives au trafic et de localisation, encadrée et limitée au strict nécessaire.

2.2 Le régime juridique de conservation des données de connexions : quelles obligations ?

Le législateur français a choisi d'encadrer la mise en place d'une connexion Wi-Fi public (ou hotspot). Son régime juridique est prévu par le Code des Postes et des Communications Electroniques (CPCE).

Aussi, la France a choisi d'adopter des mesures législatives visant à créer un régime de conservation des données techniques pesant sur différents acteurs :

- Les fournisseurs d'accès à Internet ;
- Les personnes qui, au titre d'une activité professionnelle principale ou accessoire, offrent au public une connexion permettant une communication en ligne par l'intermédiaire d'un accès au réseau, y compris à titre gratuit.

Ce régime figurant à l'article L34-1 du CPCE, prévoit une durée de conservation d'un an pour les données techniques.

Les personnes sur lesquelles pèse l'obligation de conservation des données techniques, encourent jusqu'à un an d'emprisonnement et 75 000€ d'amende en cas de non-conservation de ces données.[2] Pour les personnes morales, l'amende encourue s'élève à 375 000€[3].

En pratique, afin de limiter le risque d'accès à des sites Internet interdits par la législation française, les solutions techniques mises en place proposent souvent du filtrage d'URL. Les sites actuellement interdits d'accès par législation française s'organisent principalement autour de trois catégories :

- Les sites faisant l'apologie du terrorisme ;
- Les sites exposant des sujets pédopornographiques[4] ;
- Les sites de jeu d'argent n'ayant pas reçus d'accréditation de l'ARJEL[5].

Aujourd'hui, l'Université de Toulouse tient à jour une liste publique de catégorisation de sites, dont ceux entrants les trois catégories présentées ci-dessus propre au droit français. Cette liste est aujourd'hui de l'ordre de plusieurs millions d'URL catégorisées.

Point d'attention : L'article du Code pénal (art. 421-2-5-2 Code pénal) prévoyant le délit de consultation de site internet faisant l'apologie du terrorisme, a été abrogé le 16 décembre 2017, à la suite d'une décision du Conseil constitutionnel.

Actuellement il y a donc un vide juridique.

[2] Article L39-3 du CPCE, I 2°
[3] Article L39-3 du CPCE
[4] Article 227-23 du Code pénal
[5] Article L324-1 du Code de la sécurité intérieure (CSP)

2.3 Illustration : la commission d'une infraction pénale par l'intermédiaire d'un réseau Wi-Fi public.

La CJUE a rendu un arrêt[6], le 15 septembre 2016, traitant de l'utilisation du Wi-Fi public et des violations aux droits d'auteurs commises par les utilisateurs dudit réseau.

En l'espèce, le gérant d'un magasin proposant un accès Wi-Fi gratuit à ses clients, a été poursuivi par Sony pour le téléchargement illicite d'une œuvre musicale dont Sony détient les droits d'auteur.

La CJUE a posé, à l'occasion de cet arrêt, un principe exonérant la responsabilité de l'exploitant du magasin.

Par ailleurs, la CJUE reconnait qu'un titulaire de droits d'auteurs constatant une violation de ses droits peut demander à une juridiction nationale de faire cesser la violation ou de prévenir de telles violations.

Enfin, la Cour reconnait que la sécurisation du réseau Wi-Fi au moyen d'un mot de passe serait un moyen d'assurer l'équilibre entre les droits de propriété intellectuelle des titulaires des droits, le droit à la liberté d'entreprise des fournisseurs d'accès et enfin, le droit à la liberté d'informations des utilisateurs du réseau Wi-Fi.

Point d'attention : « L'exploitant d'un magasin qui propose gratuitement un réseau Wi-Fi n'est pas responsable des violations de droits d'auteur commises par un utilisateur.

Toutefois, un tel exploitant peut être enjoint à sécuriser son réseau par un mot de passe afin de mettre un terme à ces violations ou de les prévenir. ».

2.4 Evolutions législatives : une volonté de contrer le pseudonymat en ligne

Actuellement de nombreux débats ont lieu au sein du gouvernement, contre le pseudonymat en ligne.
En effet, la doctrine semble tendre vers une levée progressive de l'anonymat sur les plateformes.

Une proposition de loi, déposée le 6 mars 2019[7], et ayant vocation à modifier la loi pour la confiance en l'économie numérique (LCEN), propose un nouveau régime juridique visant à améliorer les procédures d'identification en ligne.

L'article 2 de cette proposition de loi envisage notamment de modifier les obligations pesant sur les hébergeurs de site internet comme suit : *« Pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales, les personnes mentionnées au 2 du I, dont l'activité dépasse un seuil de nombre de connexions défini par décret, doivent exiger de chaque utilisateur souhaitant accéder à leurs*

[6] CJUE, 15 septembre 2016, Tobias Mc Fadden
[7] Proposition de loi n°1745 du 6 mars 2019 visant à lutter contre les injures commises notamment en raison de l'appartenance à une religion

service la fourniture d'un document attestant de leur identité ainsi que la fourniture d'une déclaration de responsabilité pour les contenus qu'il diffuse ;
L'autorité judiciaire peut requérir communication auprès des prestataires mentionnés aux 1 et 2 du I des documents mentionné au précédent alinéa ».

Cette volonté de réformer les procédures d'identification en ligne est liée au manque d'efficacité des procédures en place, prévues par le Code des postes et communications électroniques (CPCE). Aujourd'hui la procédure d'identification en ligne repose sur deux acteurs distincts : les FAI et les opérateurs de communications électroniques et enfin, les personnes proposant au public, une connexion Wi-Fi.
Le projet de loi évoqué ci-dessus propose de faire peser sur les gestionnaires de plateformes en ligne, une nouvelle obligation : celle d'exiger de l'utilisateur, qu'il prouve son identité, avant de pouvoir utiliser les services proposés par la plateforme.

3 La position d'Almond

Tout d'abord, concernant la différence à faire entre un service Wi-Fi invité et un service Wi-Fi public dans le cadre de l'obligation légale de conservation des données techniques, nous considérons qu'un service Wi-Fi invité est soumis au même régime juridique qu'un service Wi-Fi public.
La raison à cette position tient principalement dans la définition d'un Etablissement Recevant du Public (ERP), qui précise uniquement qu'un ERP est définit par sa capacité à recevoir *« des personnes extérieures ».* Un environnement d'entreprise classique recevant des fournisseurs, des clients, ou des partenaires, pourrait alors s'associer à un ERP de type W[8].
Dès lors qu'une entreprise peut accueillir au sein de ses locaux des tiers, nous conseillons de respecter les obligations et bonnes pratiques décrites dans le présent document, pour le service Wi-Fi invité.

Au regard des informations techniques et légales fournies précédemment, nous conseillons de choisir des solutions permettant de stocker les informations suivantes :

1. La **date précise de la première requête** à un nouveau site web (date, heure, minute, seconde, indexé sur un serveur de temps fiable type NTP) ;
2. La **date précise de la déconnexion** au même site web ;
3. L'**adresse MAC** de l'équipement de l'utilisateur s'étant connecté au réseau ;
4. L'**adresse IP privée** au sein du réseau interne fournie à l'interface réseau de l'équipement de l'utilisateur ;
5. L'adresse **URL du site web visité** par l'utilisateur ;
6. Les informations d'**identification de l'utilisateur** fournies lors de l'enregistrement auprès du portail captif : mail, numéro de téléphone, nom, prénom, que ce soit directement ou via le lien d'authentification via Facebook, Twitter, Instagram ou tout autre service tierce.

Ces informations sont à stocker dans des bases de données sécurisées avec limitation et contrôle des accès (Separation of Duty). Ces données doivent être **conservées pour une durée d'un an** à partir de la date de génération de celles-ci, lors de la première connexion de l'utilisateur au service.

Enfin, nous conseillons de mettre en place un filtrage d'URL afin de limiter l'accès aux sites faisant partie des catégories mentionnées dans ce document :

- Les sites faisant l'apologie du terrorisme ;
- Les sites exposant des sujets pédopornographiques ;
- Les sites de jeu d'argent n'ayant pas reçus d'accréditation de l'ARJEL.

Le fournisseur responsable du service doit faciliter autant que possible les procédures de réquisitions judiciaires.

[8]https://www.service-public.fr/professionnels-entreprises/vosdroits/F32351

4 Annexes

4.1 Fiche réflexe sur la procédure de réquisition judiciaire

Le régime de communication des données techniques pesant sur les personnes offrant une connexion Wi-Fi public est prévu par l'article 60-2 du Code de procédure pénale.

Objectifs

- Comprendre la procédure de réquisition judiciaire des données techniques ;
- Déterminer les responsables en interne en cas de réquisition judiciaire.

QUAND INTERVIENT LA PROCEDURE DE REQUISITION JUDICIAIRE ?
La procédure de réquisition administrative intervient pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales.

QUELLES DONNEES DOIVENT ETRE COMMUNIQUEES ?
Les personnes proposant une connexion Wi-Fi au public, doivent communiquer les données techniques suivantes : ○ Les informations permettant d'identifier l'utilisateur ; ○ Les données relatives aux équipements terminaux de communication utilisés ; ○ Les caractéristiques techniques ainsi que la date, l'horaire et la durée de chaque communication ; ○ Les données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs ; ○ Les données permettant d'identifier le ou les destinataires de la communication.
Dans quel cas transmettre ces données ?
A la suite d'une demande adressée par l'officier de police judiciaire. ⚠ L'officier de police judiciaire dispose d'une autorisation délivrée par ordonnance du juge des libertés et de la détention.
Comment transmettre ces données ?
Ces données doivent être *« transmises par voies télématiques ou informatiques dans les meilleurs délais ».*
Qui doit transmettre ces données ?
Ces données doivent être transmises par [nom du DPO de l'organisme ou du référent DCP] dans un délai n'excédant pas 72 heures[9].
Comment obtenir remboursement des surcoûts pour la fourniture des données techniques en cas de réquisition judiciaire ?

[9] Aucun délai précis n'est indiqué dans le Code des procédures pénales, il est noté « dans les meilleurs délais ». Nous proposons un délai de 72 heures qui nous semble raisonnable, mais qui reste à adapter suivant le contexte.

Pour obtenir le remboursement des frais de production et de fourniture des données techniques (voir liste ci-dessus), il est nécessaire d'apporter toutes factures ou justificatifs disponibles.

Il convient ensuite de se référer à l'article A43-9 du Code de procédure pénale détaillant le montant hors taxe remboursé, pour chaque prestation demandée dans le cadre d'une réquisition.

4.2 Cas des services Cloud de Portail Captif

Dans de nombreux cas, les entreprises ne souhaitent pas traiter par elles-mêmes les problématiques des accès Wi-Fi publics, que ce soit pour des raisons techniques de mise en place ou de maintien de solution, ou pour des raisons de responsabilité juridique. Par conséquent, celles-ci peuvent choisir de transférer la responsabilité de la conservation des données, à un tiers.

Il existe alors quelques fournisseurs de service Wi-Fi Hotspot, principalement dans le Cloud (mais pas seulement, le service peut être rendu sous forme d'infogérance) qui proposent de fournir ce service d'accès à Internet pour du public, muni de briques optionnelles d'identification, de rétention de logs, ou encore de plus-value de type Business Intelligence sur les données collectées.

La représentation des échanges techniques qui ont alors lieu entre les équipements utilisateurs (clients) et les sites auxquels ils souhaitent accéder peuvent se présenter ainsi.

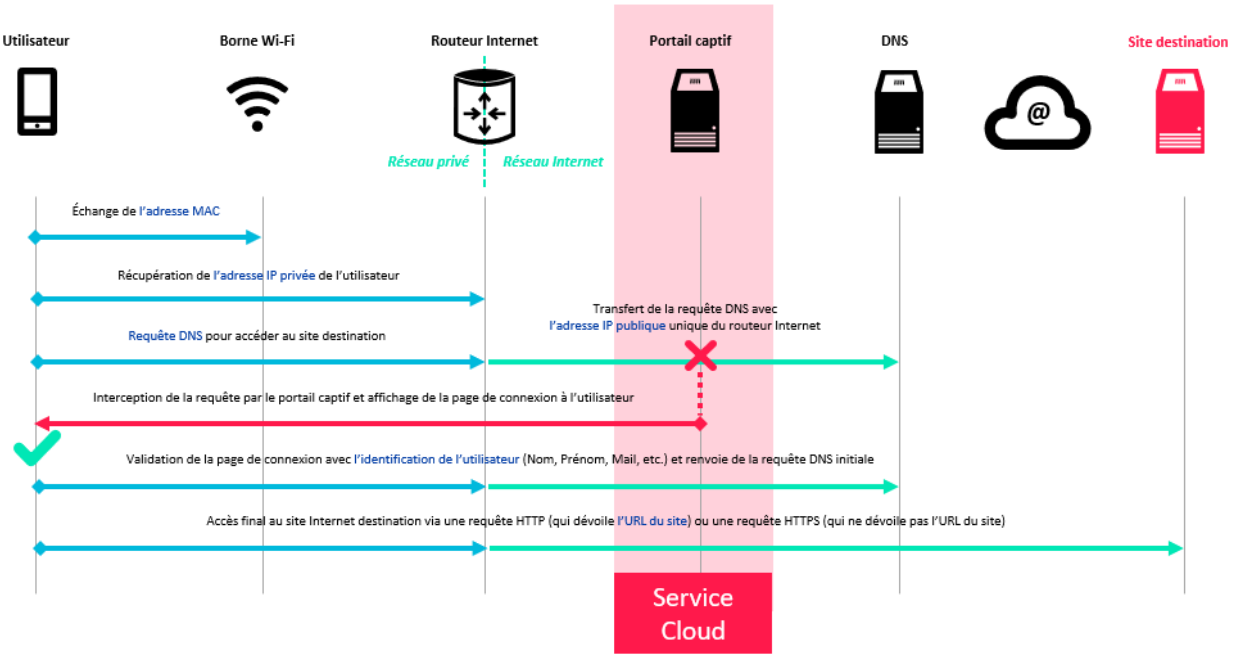

Schéma 3: Représentation des échanges simplifiés d'un service Hotspot fourni par un tiers de type Cloud

La brique de Portail Captif peut alors être considérée comme étant à l'extérieur du Système d'Information de l'entreprise puisque fournie par un tiers, qui possède dans ce cas une partie des informations de connexions des utilisateurs du service : l'adresse IP publique, les requêtes DNS, les identifications, ainsi que les URL des sites accédés.

Point d'attention : Afin de pouvoir répondre correctement aux procédures de réquisition judiciaire, deux cas se présentent lorsqu'un service Cloud est souscrit par l'entreprise :

1. La responsabilité juridique a pour objectif d'être portée par l'entreprise, alors :
    a. Il est nécessaire de formaliser la rétrocession des informations techniques depuis le service Cloud vers le Système d'Information afin de posséder toutes les informations techniques dans leur ensemble ;
    b. Il est nécessaire de centraliser toutes les informations techniques de connexion et de valider le fait qu'il est possible de recouper correctement les informations provenant du SI et du service Cloud ;
    c. Le contrat avec la société fournissant le service Cloud doit être clair quant à la répartition des responsabilités (légales et techniques) et les processus de rapatriement des données techniques doivent être formalisés.
2. La responsabilité juridique a pour objectif d'être portée par la société fournissant le service Cloud, alors :
    a. À l'inverse du cas précédent, l'entreprise se doit de formaliser la fourniture des informations techniques depuis son SI à destination du prestataire de service Cloud ;
    b. Il est nécessaire de vérifier que la société de service Cloud est en capacité à recouper l'ensemble des informations de connexion ;
    c. Le contrat avec la société fournissant le service Cloud doit être clair quant à la répartition des responsabilités (légales et techniques) et les processus de fourniture des données techniques doit être formalisé.

4.3 F.A.Q

Lors d'échanges HTTPS, qui constituent maintenant la norme, comment collecter les données techniques relatives aux URL accédées par l'utilisateur, puisque cette donnée est chiffrée par le protocole ? L'inspection profonde (DPI) des échanges pour y retrouver ces informations techniques est-elle légale ?

En effet, l'URL accédée est chiffrée lors d'une requête HTTPS (qui constitue aujourd'hui presque 80% du trafic web), ce qui empêche de récupérer et stocker cette information sans inspecter au-delà de l'en-tête des paquets : l'inspection du contenu du corps des paquets, surtout s'ils sont chiffrés, se nomme le DPI. Pour être réalisée cette technique peut s'orienter vers deux choix : soit forcer le déchiffrement du paquet, qui constitue une attaque en bonne et due forme, soit intercepter le paquet, usurper l'identité du site destination, le déchiffrer, l'analyser, le rechiffrer, puis l'envoyer à la destination légitime. Cette deuxième technique s'associe à une attaque de type Man-in-the-Middle avec usurpation d'identité. Cependant il n'existe pas de loi claire permettant de proscrire ce genre de pratique en entreprise à condition que les employés soient informés. Cette pratique entraine aussi des implications importantes vis-à-vis du RGPD. Pour ce qui est des réseaux Wi-Fi public, la mise en place de ce genre de solution est déconseillée car les équipements des

utilisateurs ne sont pas maitrisés par l'entreprise : les navigateurs détecteront "l'attaque" et afficheront une page d'alerte de sécurité.

4.3.1.1 Il existe alors deux possibilités pour récupérer l'URL accédée par les utilisateurs en dehors des requêtes HTTPS :

1. Utiliser une solution qui permet de récupérer cette information au sein des requêtes DNS initiales ;
2. Utiliser une solution capable d'analyser les échanges qui permettent l'établissement de la session TLS du HTTPS, lorsque les certificats sont échangés, afin d'y lire l'URL du site destination dans le champ Server Name Indication (SNI) du certificat.

Une pratique se démocratise pour les utilisateurs : l'utilisation du protocole de chiffrement des requêtes DNS, le DNS over HTTPS (DoH) qui chiffre donc la requête de résolution du nom de domaine du site accédé. Comment récolter les informations techniques de l'URL accédée dans ce cas ?

Si la solution choisie par l'entreprise (ou le prestataire de service Cloud) s'appuie sur les requêtes DNS pour récupérer l'information des URL accédées par les utilisateurs, l'usage du DoH pose en effet un problème car il n'existe pas de solution permettant de passer outre.

L'autre problème induit par cet usage est le filtrage d'URL : il devient alors impossible d'empêcher une connexion aux catégories de sites frauduleux dont nous avons parlé par les techniques de filtrage classique s'appuyant sur des blacklist d'URL.

Même question pour la démocratisation de l'utilisation des champs SNI chiffrés dans les certificats (ESNI) ?

Le champ SNI permet principalement d'héberger plusieurs sites en HTTPS avec la même adresse IP publique. Le champ SNI sert alors à "orienter" la requête vers le bon site destination : il contient le nom de domaine du site. Le champ SNI chiffré a été introduit par CloudFlare et Mozilla, nommé le ESNI. Cette pratique permet donc de chiffrer le contenu de ce champ, et ainsi de rendre illisible l'URL accédée *in fine* par l'utilisateur.

De même, il n'existe actuellement pas de technique pour pouvoir malgré tout lire l'URL par ce moyen lorsque l'ESNI est utilisé.

Que faire des données techniques lorsque l'utilisateur passe par un service de Proxy ou de VPN, auquel cas il est impossible de récupérer les informations de l'URL réellement accédée et de durée de connexion à celle-ci ?

L'usage d'un proxy ou d'un VPN par l'utilisateur sur un réseau Wi-Fi publique reste une pratique recommandée pour les utilisateurs afin de garantir la sécurité de leurs échanges, cependant le fournisseur du service ne pourra en effet récupérer que les informations de connexion au service Proxy ou VPN.

Dans ce cas, de notre point de vue, l'obligation légale du fournisseur de service se limite à conserver les informations de connexion "visible", c'est à dire la connexion au service Proxy ou VPN (URL accédée, date de connexion, de déconnexion, adresses IP, etc.). Autrement nous conseillons de désactiver la possibilité de se connecter autrement qu'en HTTP et HTTPS pour le public (restreindre aux ports TCP-80 et TCP-443.

Contacts pour ce livre blanc
Adrien Gaillard
Léa Thomas
E. agaillard@almond.consulting
E. lthomas@almond.consulting

Paris | Nantes | Strasbourg

almond.consulting