DELIBERATION N° 2013-121 DU 21 OCTOBRE 2013 DE LA COMMISSION DE CONTROLE DES INFORMATIONS NOMINATIVES PORTANT RECOMMANDATION SUR L'INSTAURATION DE REGLES INTERNES RELATIVES A LA PROCEDURE D'ALERTE EN CAS DE VIOLATION DE DONNEES A CARACTERE PERSONNEL PAR LES ORGANISMES MONEGASQUES - PRESTATAIRES DE SERVICE OU SOUS-TRAITANT - DE FOURNISSEURS DE SERVICES DE COMMUNICATIONS ELECTRONIQUES SOUMIS A LA LEGISLATION EUROPEENNE

Vu la Constitution du 17 décembre 1962 ;

Vu la Convention 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 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° 1.299 du 15 juillet 2005 sur la liberté d'expression publique ;

Vu la Loi n° 1.383 du 2 août 2011 sur l'économie numérique ;

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, susvisée ;

Vu le Règlement (UE) n° 611/2013 de la Commission européenne du 24 juin 2013 concernant les mesures relatives à la notification des violations de données à caractère personnel en vertu de la Directive 2002/58/CE du Parlement européen et du Conseil sur la vie privée et les communications électroniques ;

La Commission de Contrôle des Informations Nominatives,

Préambule

Conformément à l'article 1er de la loi n° 1.165 du 23 décembre 1993, modifiée, les traitements automatisés ou non automatisés d'informations nominatives ne doivent pas porter atteinte aux libertés et droits fondamentaux consacrés par le Titre III de la Constitution.

La Commission de Contrôle des Informations Nominatives, autorité administrative indépendante, a pour mission de veiller au respect de ces dispositions. A ce titre, elle est notamment habilitée, aux termes de l'article 2 de la loi n° 1.165, précitée, à formuler toutes recommandations entrant dans le cadre des missions qui lui sont conférées par ladite loi.

Par la présente recommandation, la Commission estime opportun d'appeler l'attention des responsables de traitement sur l'entrée en vigueur, le 25 août 2013, du Règlement n° 611/2013 de la Commission européenne concernant les mesures relatives à la notification des violations de données à caractère personnel en vertu de la Directive 2002/58/CE du Parlement européen et du Conseil sur la vie privée et les communications électroniques.

Ce nouveau Règlement, d'application directe sur le territoire de l'Union européenne (UE), intervient dans un contexte d'harmonisation des procédures de notification.

Nouvelles règles spécifiques pour la protection des consommateurs européens en cas de perte ou de vol de données électroniques à caractère personnel, certains principes de ce Règlement s'appliquent aux opérateurs de services de télécommunications et aux fournisseurs de services internet (ISP) monégasques, dès lors que ces derniers sont prestataires de service ou sous-traitants d'une société établie sur le territoire d'un Etat membre de l'UE.

A cet égard, la Commission rappelle qu'afin de faciliter les échanges de données personnelles entre l'Union européenne et la Principauté de Monaco, le Gouvernement Princier a déposé, le 9 novembre 2009, auprès de la Commission européenne une demande aux fins de faire constater l'adéquation de la législation monégasque à la réglementation européenne, laquelle protège rigoureusement les données personnelles de ses ressortissants.

Dans ce contexte, et au-delà même de leurs propres intérêts économiques, il apparaît essentiel que les organismes monégasques concernés se plient aux nouvelles règles européennes afin d'une part, de conserver ou de développer leur clientèle européenne, et d'autre part, de ne pas être un frein à l'obtention de la « *protection adéquate* » par la Principauté, et le cas échéant, ne pas mettre en péril le maintien de cette reconnaissance qui ne sera jamais un acquis.

I. <u>Dispositions Générales</u>

La Commission rappelle qu'aux termes de l'article 11 alinéa 2 de la loi n° 1.299 du 15 juillet 2005 sur la liberté d'expression publique, « *On entend par communication électronique toute transmission, émission ou réception de signes, de signaux, d'écrits, d'images, de sons ou de renseignements de toute nature par fil, optique, radioélectricité ou autres systèmes électromagnétiques* ».

La dimension transnationale de ce secteur, illustrée par les Services de l'Internet, de l'économie numérique ou de la téléphonie mobile, fait peser des risques non négligeables sur les informations nominatives de leurs utilisateurs : vol d'informations, usurpations d'identité, cambriolages facilités, réputation entachée, pratiques commerciales abusives (...).

Aussi, l'encadrement progressif du traitement des informations nominatives lors des opérations nécessaires au fonctionnement de l'ensemble de ces Services de communications électroniques apparaît comme une évidence.

II. Sur les informations nominatives collectées

La Commission relève que les fournisseurs de services de communications électroniques (ex. opérateurs de télécommunications, fournisseurs de services Internet ainsi que leurs prestataires de service ou sous-traitants) détiennent nombre de données personnelles dont il est impossible de dresser une liste exhaustive.

Peuvent toutefois être citées, à titre d'exemple, les données suivantes :

- une dénomination, un nombre, une adresse fournie par celui qui émet la communication ou qui utilise une connexion pour effectuer la communication ;
- les données permettant l'identification de l'abonné ou de l'utilisateur individuel qui reçoit un service de radiodiffusion fourni sur un réseau public de communication dans le cas de la fourniture de services de type vidéo à la demande ;
- les données nécessaires à l'identification d'un client et des prestations objets d'une transaction de type commercial, voire à la preuve de la transaction ;
- les données nécessaires à l'efficacité de la conception des sites des fournisseurs de communications électroniques, permettant de faciliter la fourniture des services de la société de l'information, voire de plus en plus souvent de valider l'identité de l'utilisateur du service ;
- des informations traitées par les services à valeur ajoutée permettant, par exemple, de disposer de conseils sur les forfaits tarifaires les plus avantageux, le guidage routier, les informations sur l'état de la circulation, des prévisions météorologiques ou des informations touristiques ;
- des données relatives au trafic permettant la transmission de la communication électronique sur le réseau, que sont le routage, la durée, le moment ou le volume d'une communication, le protocole de référence, l'emplacement des équipements terminaux de l'expéditeur ou/et du destinataire, l'identification du réseau de départ ou d'arrivée de la communication, le début, la fin ou la durée de la communication, le format dans lequel la communication est acheminée par le réseau. Ces informations font ainsi l'objet d'un stockage automatique, intermédiaire et transitoire car nécessaire à la transmission de la communication au sein du réseau ou entre réseaux ;
- des données de localisation permettant de déterminer où se situe ou se situait à un moment donné un équipement terminal par la latitude, la longitude et l'altitude du lieu où il se trouve ou se trouvait, la direction du mouvement, l'identification de la cellule du réseau ou encore le moment auquel l'information sur la localisation a été enregistrée.

Ainsi les données traitées sur les abonnés ou les utilisateurs de réseaux de communications électroniques par les fournisseurs des services de communications électroniques pour établir des connexions, transmettre des communications ou répondre à une demande, fournir un service spécifique, établir une facturation, permettre un paiement en ligne, réaliser des démarches en ligne (…), contiennent des informations, directement ou indirectement nominatives, touchant à leur vie privée, parfois au principe du secret des correspondances.

III. Sur l'existence d'une obligation de sécurité renforcée

La Commission constate que la règlementation européenne, dont sont issus les principes de la présente délibération, renforce l'obligation de sécurité incombant aux responsables de traitement et à leurs sous-traitants ou prestataires de service en ce qui concerne l'exploitation de données personnelles d'origine européenne.

A cet égard, elle relève que les fournisseurs de services de communications électroniques sont soumis à des obligations spécifiques notamment fixées par la Directive 2002/58/CE, modifiée, du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (Directive dite « *vie privée et communications électroniques* »).

Elle impose au sein de son article 4, intitulé « *sécurité du traitement* », la mise en place de mesures techniques et organisationnelles afin de garantir la sécurité des services de communications électroniques, la mise en place de procédures préventives et correctives en cas de violation de la sécurité du réseau, la tenue d'un inventaire des violations de données à caractère personnel, ainsi que l'information de l'autorité de protection des données compétentes sur le territoire de l'Union européenne, voire des abonnées ou des particuliers utilisateurs des services lorsque cette violation présente un risque ou est de nature à affecter négativement leurs données à caractère personnel ou leur vie privée.

Les modalités de notification de l'autorité de protection des données compétente ont été précisées dans le Règlement européen n° 611/2013. Son considérant 18 prend également en compte le recourt à la sous-traitance.

Ainsi, il précise que si le fournisseur de service de communications électroniques « *recourt à un autre fournisseur pour assurer une partie du service, par exemple en ce qui concerne la facturation ou des tâches de gestion, cet autre fournisseur, qui n'est pas directement lié par contrat avec l'utilisateur final, ne devrait pas être tenu de notifier les violations de données à caractère personnel. En revanche, il devrait alerter et informer le fournisseur avec lequel il est directement lié par contrat. Cela devrait également valoir dans le cadre de la fourniture en gros de services de communications électroniques, lorsque le fournisseur en gros n'est en général pas directement lié par contrat avec l'utilisateur final* ».

Les obligations qui doivent peser sur cet autre fournisseur (prestataire de service) sont de la sorte fixées à l'article 5 dudit Règlement : « *Lorsque, pour fournir une partie du service de communications électroniques, il est fait appel à un autre fournisseur qui n'est pas directement lié par contrat avec les abonnés, cet autre fournisseur informe immédiatement celui qui l'a engagé en cas de violation de données à caractère personnel* ».

L'obligation de notification des violations de données à caractère personnel n'étant pas prévue par la législation monégasque, aucune notification ne devra être effectuée auprès de la CCIN.

Toutefois, dans le contrat qui les lie à leur client européen, les organismes monégasques se devront de respecter les obligations imposées à leur client par le Règlement européen aux risques de perdre leurs marchés.

IV. <u>Sur les mesures techniques et organisationnelles devant impérativement être mises en place</u>

A titre liminaire, la Commission rappelle aux organismes monégasques concernés que la soumission de leurs traitements automatisés d'informations nominatives aux formalités de la loi n° 1.165 est un préalable indispensable au respect de la réglementation européenne.

Par ailleurs, la Commission tient également à rappeler la nature des mesures techniques et organisationnelles que doivent mettre en place les organismes monégasques s'inscrivant dans une relation de sous-traitance afin d'alerter et d'informer leur client (responsables de traitement européens) des violations de données à caractère personnel qu'ils auront constatées.

Tout d'abord, elle tient à préciser que ces alertes devraient être réalisées dans les plus brefs délais tenant compte des impératifs de leur client européen, qui dispose d'un délai de vingt-quatre heures après le constat de la violation pour la notifier à l'autorité de protection des données à caractère personnel dont il relève, et « *sans retard injustifié à leur abonné ou au particulier* » concerné.

Ainsi, selon la nature des opérations effectuées en Principauté et la connaissance des informations nominatives traitées pour le compte de leur client telles qu'évoquées au point III de la présente délibération, les mesures techniques et organisationnelles devraient :

- être fondées sur des procédures internes écrites permettant de veiller à la qualité, à la transparence, à la lisibilité des mesures dans le prolongement des principes QoS (Qualité of Services) ;

- être établies en tenant compte des risques présentés par le traitement et de la nature des informations traitées ;

- permettre d'identifier les violations de données à caractère personnel et de déterminer si cette violation est susceptible de porter atteinte aux données elles-mêmes ou à la vie privée des personnes concernées, notamment s'il s'agit de données financières, de données de santé, ou de toutes informations encadrées par les articles 11, 11-1 et 12 de la loi n° 1.165, ou encore de certaines données spécifiquement liées à la fourniture de services de téléphonie et Internet, c'est-à-dire les données relatives au courrier électronique, les données de localisation, les fichiers journaux, les historiques des sites consultés et les listes d'appel détaillées (selon le considérant 12 du Règlement) ;

- permettre de déterminer les circonstances de la violation de données à caractère personnel, en particulier :
  - la date et l'heure de l'incident (si elles sont connues ou une estimation dans le cas contraire) et du constat de l'incident ;
  - la nature de l'incident (ex. perte, vol, reproduction), la nature et la teneur des données (si l'organisme en a la connaissance) ;
  - l'endroit où les données ont subi l'incident (y compris le lieu physique de la violation et le moyen de traitement concerné) ;
  - le cas échéant, le moment à partir duquel il peut être établi que les données sont en possession d'un tiers non autorisé ;

- mettre en évidence, si c'est le cas, les mesures de protection technologiques mises en œuvre et appliquées aux données les rendant incompréhensibles à toute personne qui n'est pas autorisée à y avoir accès, tenant compte de l'article 4 chiffre 2 du Règlement ;

- mettre en évidence les mesures techniques et organisationnelles correctives mises en place pour mettre fin et/ou atténuer les préjudices potentiels ;

- établir des contrôles afin de comprendre pourquoi les violations de données à caractère personnel se sont produites et les risques résiduels ;

- permettre de suivre la procédure d'alerte activée en conservant la date et l'heure de chaque communication d'information, l'identité et la fonction de chaque personne alertée, les éléments communiqués, ainsi que les réponses du client fournisseur de services.

Considérant les impératifs de traçabilité en matière de sécurité, la Commission recommande que les organismes monégasques concernés mettent en place un inventaire des violations des données à caractère personnel constatés reprenant, pour chaque client fournisseur de services de communications électroniques, notamment, leurs circonstances, leurs effets et les mesures prises pour y remédier.

Elle précise enfin qu'il n'appartient pas à l'organisme monégasque d'établir les conséquences vraisemblables de la violation des données à caractère personnel constatée pour les personnes physiques impactées, notamment les cas où la violation pourrait entraîner un vol ou une usurpation d'identité, une atteinte à l'intégrité physique, une souffrance psychologique, une humiliation ou une atteinte à la réputation, évoquées à l'article 3 point 2 chiffre b du Règlement.

Toutefois, la prise en considération des impacts pour les personnes physiques devrait être une composante fondamentale des mesures techniques et organisationnelles mises en place.

En conclusion, la Commission précise que tant que la législation monégasque en matière de protection des informations nominatives n'aura pas été reconnue par l'Union européenne comme disposant d'un niveau de protection adéquat, les communications et transferts d'informations nominatives à partir de l'Union européenne vers la Principauté de Monaco sont susceptibles d'être soumis dans les pays de l'Union à des formalités autorisant le transfert des données. A ce titre, les mesures prises pour assurer la sécurité des informations nominatives et de leur traitement, comme celles développées plus avant, sont des facteurs incontournables examinés par les autorités européennes compétentes pour autoriser ou refuser lesdits transferts. Une fois cette protection adéquate obtenue, ces mesures devront conserver un haut niveau de fiabilité en considération des impératifs de la loi n° 1.165 mais également tenant compte du caractère réversible de la décision d'adéquation de l'Union européenne.

Après en avoir délibéré,

Invite les organismes monégasques concernés :

- **à se rapprocher de leurs clients, fournisseurs de services de communications électroniques européens, afin de déterminer les procédures qui devront être mises en place dans le cadre de l'application de ce Règlement européen ;**

- **à veiller à la conformité de leurs traitements automatisés au regard des dispositions de la loi n° 1.165 du 25 décembre 1993, modifiée.**

Le Président,

Michel Sosso