Délibération n° 2022-096 du 20 juillet 2022

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

« *Surveillance et analyse des flux internet entrants et sortants sécurisés, par le protocole cryptograhique connu sous le nom de « Secure Socket Layer » (SSL)* »

présenté par Barclays Bank PLC (succursale de Monaco)

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 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° 1.338 du 7 septembre 2007 sur les activités financières, modifiée ;

Vu l'Ordonnance Souveraine n° 1.284 du 10 septembre 2007 portant application de la Loi n° 1.338 du 7 septembre 2007 sur les activités financières, modifiée, susvisée ;

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 la délibération n° 2011-82 du 21 octobre 2011 de la Commission de Contrôle des Informations Nominatives portant recommandation sur les principes européens applicables aux traitements automatisés ou non automatisés d'informations nominatives ;

Vu la demande d'autorisation déposée par Barclays Bank PLC (succursale de Monaco) le 28 avril 2022 concernant la mise en œuvre d'un traitement automatisé d'informations nominatives ayant pour finalité *« Surveillance des flux internet entrants et sortants sécurisés, par le protocole cryptograhique connu sous le nom de « Secure Socket Layer » (SSL)* » ;

Vu la prorogation du délai d'examen de la présente demande d'autorisation notifiée au responsable de traitement le 27 juin 2022, conformément à l'article 11-1 de la Loi n° 1.165 du 23 décembre 1993 ;

Vu le rapport de la Commission de Contrôle des Informations Nominatives en date du 20 juillet 2022 portant examen du traitement automatisé susvisé.

La Commission de Contrôle des Informations Nominatives,

Préambule

Barclays Bank PLC est une société anglaise établie à Monaco par sa succursale enregistrée au RCI sous le numéro 68S01191, ayant pour activité « *la réalisation de toutes opérations de banque et connexes, telles que définies par la Loi bancaire* ».

Afin de filtrer les contenus potentiellement dangereux ou d'identifier les données confidentielles qui ne doivent pas être divulguées, cette société souhaite mettre en place une surveillance appelée « *Inspection SSL* » qui consiste en l'interception des communications Internet cryptées (HTTPS) entre ses « *clients* » (clients, prospects, prestataires et employés) et le serveur pour les scanner.

Le traitement objet de la présente demande permet de surveiller les accès au système d'information, il relève donc du régime de l'autorisation préalable visé à l'article 11-1 de la Loi n° 1.165 du 23 décembre 1993.

I. Sur la finalité et les fonctionnalités du traitement

Le responsable de traitement indique que le traitement a pour finalité « *Surveillance des flux internet entrants et sortants sécurisés, par le protocole cryptograhique connu sous le nom de « Secure Socket Layer » (SSL) ».*

Les personnes concernées sont les employés, les clients, les prospects et les prestataires.

Enfin, les fonctionnalités de ce traitement vont permettre d' « *étendre la surveillance existante effectuée pour l'ensemble des communications du Groupe à celle des flux internet entrants et sortants sécurisés par le protocole SSL »* couvrant la succursale à Monaco.

A cet égard, la Commission prend note que « *Cette surveillance appelée « Inspection SSL » consiste en l'interception des communications cryptées (HTTPS) entre le « client »* [clients, prospects, prestataires et employés] *et le serveur pour les scanner dans le but de filtrer les contenus potentiellement dangereux ou d'identifier les données confidentielles qui ne doivent pas être divulguées ».*

Elle relève également qu'« *Il s'agit d'une mesure de sécurité supplémentaire, car en plus des informations légitimes, un contenu malveillant pourrait également être caché dans le trafic crypté, ou un initié pourrait essayer d'exfiltrer des informations de la banque* ».

La Commission rappelle toutefois que tout traitement d'informations nominatives doit avoir une finalité « *déterminée, explicite et légitime* » aux termes de l'article 10-1 de la Loi n° 1.165 du 23 décembre 1993.

En l'espèce, la finalité du présent traitement doit être plus explicite c'est-à-dire être claire et précise pour les personnes concernées en indiquant que ces flux entrants et sortants sont également analysés afin d'appliquer des scripts conçus pour détecter les logiciels malveillants entrants ou les fuites de données .

Par conséquent, elle modifie la finalité comme suit : « *Surveillance et analyse des flux internet entrants et sortants sécurisés, par le protocole cryptograhique connu sous le nom de « Secure Socket Layer » (SSL)* ».

II. Sur la licéité et la justification du traitement

Le responsable de traitement indique que le traitement est justifié par « *la réalisation d'un intérêt légitime poursuivi [par lui et qui] ne méconnait ni l'intérêt, ni les droits et libertés fondamentaux de la personne concernée* ».

A cet égard, la Commission observe que le responsable de traitement utilise « *les journaux Web pour identifier les activités malveillantes telles que le traffic de commande et de contrôle, les visites de sites d'hameçonnage, etc. S'il y a des indications qu'un membre du personnel est complice, cela sera transmis à l'équipe 'Investigations*' ».

Elle prend note que « *Dans la grande majorité des cas, le membre du personnel est une victime et, par conséquent, tout ce qui préoccupe [le responsable de traitement] est le risque que la banque de l'organisation soit piratée* ».

Enfin, elle relève que « *La capacité rapide à identifier un collègue ou une machine qui a été compromise est importante pour protéger la vie privée de la banque et de [ses] clients » et que « Toute catégorie de sites peut être utilisée abusivement par des attaquants et il y a de plus en plus de cas où des catégories qui sont souvent exclues de la surveillance pour des raisons de confidentialité sont utilisées abusivement pour contrôler les contrôles de sécurité* ».

La Commission considère ainsi que le traitement est justifié, conformément aux dispositions de l'article 10-2 de la Loi n° 1.165 du 23 décembre 1993.

III. Sur les informations nominatives traitées

Le responsable de traitement indique que les informations nominatives traitées sont :

- identité : nom et prénom de l'employé, nom et prénom de la personne à contacter et société pour les clients, prospects et prestataires ;
- données d'identification électronique : adresse email professionnelle, nom, prénom et nom d'utilisateurs de l'employé, adresse email des clients, prospects et prestataires ;
- infractions : recherches complémentaires accomplies, à savoir les fichiers journaux pour la détection des malwares et le contenu de l'email et de toutes les éventuelles pièces jointes pour les fuites de données ;
- informations temporelles : date et heure de l'email contenant le lien internet ou de sa recherche Internet pour l'employé, date et heure de l'email contenant le lien internet pour les clients, prospects et prestataires ;
- liens HTTPS fréquentés lors de recherches internet et éventuel(s) document(s) téléchargé(s) depuis l'internet.

Les informations ont pour origine les flux web sortants pour les employés et les flux web entrants pour les clients, prospects et prestataires.

La Commission considère ainsi 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 effectuée par le biais des Conditions Générales pour les clients, de la charte informatique pour les employés et des Contrats de service pour les prestataires.

L'ensemble de ces documents n'ayant pas été joints à la demande, la Commission rappelle que ceux-ci doivent impérativement comporter l'ensemble des mentions prévues à l'article 14 de la Loi n° 1.165 du 23 décembre 1993.

Elle rappelle par ailleurs que l'information préalable doit être effectuée auprès de l'ensemble des personnes concernées par le traitement dont s'agit, et donc y compris auprès des prospects.

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

Le responsable de traitement indique que le droit d'accès s'exerce sur place, par voie postale ou par courrier électronique.

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.

Par ailleurs, s'agissant de l'exercice du droit d'accès par voie électronique, elle considère qu'une procédure devra être mise en place afin que le responsable de traitement puisse s'assurer que l'expéditeur du courriel est effectivement la personne concernée par les informations. A ce titre, elle précise que si une copie d'un document d'identité était demandée, la transmission et le traitement de ce document devront faire l'objet de mesures de protection particulières comme rappelé dans sa délibération n° 2015-116 du 18 novembre 2015 portant recommandation sur la collecte et la conservation de la copie de documents d'identité officiels.

Sous ces conditions, la Commission considère que les modalités d'exercice des droits des personnes concernées sont conformes aux dispositions des articles 13, 15 et 16 de la Loi n° 1.165 du 23 décembre 1993.

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

- ***Sur les destinataires***

Le responsable de traitement indique que les informations sont susceptibles d'être communiquées aux Autorités administratives et judiciaires dans le cadre de leurs missions légalement conférées.

La Commission considère que le Service d'Information et de Contrôle des Circuits Financiers (SICCFIN) et la Commission de Contrôle des Activités Financières (CCAF) peuvent, dans le cadre exclusif des missions qui leur sont conférées, être destinataires d'informations nominatives traitées.

Par ailleurs, elle estime que la communication aux Autorités judiciaires peut être justifiée par les besoins d'une enquête judiciaire. A cet égard, la Commission rappelle qu'en cas de transmission, ces Autorités ne pourront avoir accès aux informations objet du traitement, que dans le strict cadre de leurs missions légalement conférées.

Elle considère donc que de telles transmissions sont conformes aux exigences légales.

- ***Sur les personnes ayant accès au traitement***

Les personnes habilitées à avoir accès au traitement sont :

- le supérieur hiérarchique de l'employé : consultation, analyse et modification (positif/ faux positif) ;
- les équipes « *Insider Threat* » et « *Cyber Operations* » de Barclays situées au Royaume-Uni, aux Etats-Unis et en Inde : consultation et analyse initiale ;

- les équipes « *Investigations* » de Barclays Barclays situées au Royaume-Uni, aux Etats-Unis et en Inde : consultation et analyse des cas positifs uniquement.

La Commission prend acte que les équipes Cyber Sécurité, de conformité et de RH de Barclays Bank PLC Monaco ne sont pas des utilisateurs habilités puisqu'elles ne recevront que « *des informations extraites des applications Symantec en fonction de la nécessité de traiter un problème local de sécurité ou de conformité* ».

Considérant les attributions de ces personnes, et eu égard à la finalité du traitement, les accès susvisés sont justifiés.

La Commission relève toutefois que certains des destinataires des informations sont situés en Inde et aux Etats-Unis.

Aussi, ces pays ne disposant pas d'un niveau de protection adéquat au sens de la Loi n°1.165 du 23 décembre 1993, la licéité de ces communications d'informations nominatives sera analysée dans les deux demandes d'autorisation de transfert concomitamment soumises.

La Commission rappelle enfin qu'en application de l'article 17-1 de la Loi n° 1.165 du 23 décembre 1993 la liste nominative des personnes ayant accès au traitement doit être tenue à jour, et précise que cette liste doit lui être communiquée à première réquisition.

VI. Sur les interconnexions et rapprochements

Le responsable de traitement indique que le présent traitement fait l'objet de six interconnexions avec les traitements ayant respectivement les finalités suivantes :

- « Analyse des mails entrants à des fins *de défense contre les cyber attaques* » ;
- « *Mise en place d'un dispositif de surveillance, de détection et d'alerte des menaces internes à la Cybersécurité de Barclays, dénommé EXABEAM* » ;
- « *Gestion et contrôle des habilitations et des accès informatiques mis en œuvre à des fins de surveillance et de contrôle des accès au Système d'Information* » ;
- « *Gestion du personnel* » ;
- « *Gestion et supervision de la messagerie professionnelle à des fins de surveillance* » ;
- « *Détection et réponse aux attaques cyberavancées* ».

La Commission constate que ces traitements ont été légalement mis en œuvre.

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 particulière.

La Commission rappelle néanmoins que 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.

Elle précise que la copie ou l'extraction d'informations issues de ce traitement doit être chiffrée sur son support de réception.

La Commission rappelle également 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

Le responsable de traitement indique que les données sont toutes conservées 1 an.

Il précise toutefois que « *les pièces jointes sont systématiquement détachées des alertes visibles par les équipes 'Insider Threat' et 'Cyber Operations' 6 mois après la date d'ouverture de chacune des alertes pour les 'faux positifs' et les alertes pour lesquelles aucune suspicion n'avait été identifiée* » et que « *les informations référées aux équipes 'Investigations' (uniquement pour les cas de 'méfaits' avérés) sont généralement conservées pour une durée de 6 ans pouvant s'étendre jusqu'à 7 ans dans le cas d'éventuels impacts financiers pour la banque* ».

Enfin la Commission prend note « *Qu'en l'absence de rétention des alertes pour une certaine période de temps* », le responsable de traitement ne serait « *pas en mesure de calibrer et/ou d'améliorer les règles de fonctionnement des alertes* » et « *qu'il est possible de créer des critères spécifiques de purge des alertes pour un ou des pays spécifique(s) plus fréquemment* » si cela était requis.

Aussi, elle demande que les faux positifs soient immédiatement supprimés.

Par ailleurs, concernant les informations référées aux équipes '*investigations*', la Commission demande que celles-ci soient supprimées une fois leur instruction en interne clôturée.

Après en avoir délibéré, la Commission :

Modifie la finalité du traitement par « *Surveillance et analyse des flux internet entrants et sortants sécurisés, par le protocole cryptograhique connu sous le nom de « Secure Socket Layer » (SSL)* ».

Considère qu'une procédure relative au droit d'accès par voie électronique devra être mise en place afin que le responsable de traitement puisse s'assurer que l'expéditeur du courriel est effectivement la personne concernée par les informations.

Rappelle que :

- les documents d'information préalable des personnes concernées doivent impérativement comporter l'ensemble des mentions prévues à l'article 14 de la Loi n°1.165 du 23 décembre 1993 ;

- l'information préalable doit être effectuée auprès de l'ensemble des personnes concernées par le traitement dont s'agit, et donc y compris auprès des prospects ;

- la réponse à ce droit d'accès doit s'exercer dans le mois suivant la réception de la demande ;

- le SICCFIN et la CCAF peuvent, dans le cadre exclusif des missions qui leur sont conférées, être destinataires des informations du traitement ;

- les Autorités judiciaires ne peuvent avoir accès aux informations objet du traitement que dans le strict cadre de leurs missions légalement conférées ;

- la liste nominative des personnes ayant accès au traitement doit être tenue à jour et doit lui être communiquée à première réquisition ;

- 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 ;

- la copie ou l'extraction d'informations issues de ce traitement doit être chiffrée sur son support de réception.

Demande que :

- les faux positifs soient immédiatement supprimés ;

- les informations référées aux équipes '*investigations*' soient supprimées une fois leur instruction en interne clôturée.

A la condition de la prise en compte de ce qui précède,

la Commission de Contrôle des Informations Nominatives **autorise la mise en œuvre par Barclays Bank PLC (succursale de Monaco) du traitement automatisé d'informations nominatives ayant pour finalité « *Surveillance et analyse des flux internet entrants et sortants sécurisés, par le protocole cryptograhique connu sous le nom de « Secure Socket Layer » (SSL)* ».**

Le Président

Guy MAGNAN