Délibération n° 2020-012 du 15 janvier 2020

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

« *Détection et réponse aux attaques cyber avancées* »

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 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 23 octobre 2019 concernant la mise en œuvre d'un traitement automatisé d'informations nominatives ayant pour finalité *« Détection et réponse aux attaques cyber avancées* » ;

Vu la prorogation du délai d'examen de la présente demande d'autorisation notifiée au responsable de traitement le 20 décembre 2019, 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 15 janvier 2020 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 d'offrir un service et des outils de travail sécurisés à la fois à ses clients et à ses employés, cette société souhaite se doter d'un outil de détection et réponse aux attaques cyber avancées.

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 traitement a pour finalité « *Détection et réponse aux attaques cyber avancées».*

Les personnes concernées sont les « *Salariés, clients, prospects, fournisseurs* ».

Enfin, les fonctionnalités de ce traitement sont les suivantes :

- la recherche automatique d'indicateurs de compromission ;
- l'analyse des évènements critiques afin d'identifier les comportements anormaux ;
- en cas d'alerte, la fourniture d'un premier niveau d'analyse 'forensic' ;
- la mise en quarantaine du système compromis ;
- la constitution de preuves.

A cet égard, la Commission prend acte des précisions du responsable de traitement selon lesquelles les comportements anormaux ne sont pas des « *comportements au sens humain, mais au sens informatique, à savoir le type d'activités techniques qu'exécute un programme informatique donné, ou un ordinateur sur un réseau donné* ».

Elle constate ainsi 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 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 ledit traitement va permettre au responsable de traitement « *de fournir un service et des outils de travail sécurisés respectivement à ses clients et ses employés* ».

Elle relève par ailleurs que « *Le traitement d'informations nominatives par l'outil de 'Détection et réponse aux attaques cyber avancées' permet d'éviter que ces mêmes informations ne soient l'objet de cyber attaques* ».

Enfin, la Commission constate que « *les données nominatives ne sont traitées qu'en cas de suspicion raisonnable de l'existence d'une vulnérabilité ou d'une cyber attaque* », que « *des mesures additionnelles réduisent au strict nécessaire la remontée d'informations dans les alertes de sécurité* » et qu' « *aucun accès à des documents personnels ne se fera sans accord de leurs propriétaires* ».

Elle considère donc 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

Les informations nominatives traitées sont :

- données d'identification électronique : login, adresse IP, nom du poste, nom d'utilisateur ;
- alertes : toute information nominative contenue dans le nom d'un fichier ou d'un répertoire faisant l'objet d'une alerte.

Concernant les alertes, la Commission prend acte des précisions du responsable de traitement selon lesquelles « *dans le cas d'une suspicion de compromission d'un fichier* » l'outil de détection des menaces cyber avancées « *va remonter le nom du fichier concerné dans l'alerte* » mais que « *les noms des fichiers étant des champs libres, ils sont susceptibles de contenir des informations nominatives* ».

Ces informations ont pour origine la solution de détection et de réponse aux attaques cyber avancées.

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 d'une rubrique propre à la protection des données accessible en ligne et d'une procédure interne accessible en Intranet.

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.

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

Le droit d'accès s'exerce sur place, par voie postale ou par courrier électronique.

S'agissant de l'exercice du droit d'accès par voie électronique, la Commission 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 cette condition, 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 tout d'abord que les informations collectées sont communiqués aux entités du Groupe Barclays en charge du traitement des alertes situées aux Etats-Unis, en Inde et à Singapour.

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 la demande d'autorisation de transfert concomitamment soumise.

Le responsable de traitement indique par ailleurs que les informations sont susceptibles d'être communiquées à la Direction de la Sûreté Publique.

La Commission estime que la communication à la Direction de la Sûreté Publique peut être justifiée pour les besoins d'une enquête judiciaire.

A cet égard, elle rappelle qu'en cas de transmission, ladite Direction ne pourra avoir communication des informations que dans le strict cadre de ses missions légalement conférées.

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

Les personnes habilitées à avoir accès au traitement sont :

- l'équipe Technology (Monaco) : consultation et maintenance ;
- l'équipe Cyber & Information Security (Monaco): consultation.

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

La Commission rappelle toutefois 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 d'une interconnexion avec un traitement lié au système permettant de corréler des logs provenant de plusieurs sources à des fins d'identification d'incidents de sécurité.

Il appert par ailleurs à l'étude du dossier une interconnexion avec un traitement lié aux habilitations.

Ces deux traitements n'ayant pas fait l'objet de formalités auprès de la CCIN, la Commission demande au responsable de traitement de les lui soumettre dans les plus brefs délais.

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.

Elle 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

Les informations collectées sont conservées 30 jours.

La Commission considère que cette durée est conforme aux exigences légales.

Après en avoir délibéré, la Commission :

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 ;

- les Services de Police monégasque ne pourront avoir communication des 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 au responsable de traitement de lui soumettre dans les plus brefs délais le traitement lié au système permettant de corréler des logs provenant de plusieurs sources à des fins d'identification d'incidents de sécurité ainsi que le traitement lié aux habilitations.

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 « *Détection et réponse aux attaques cyber avancées* ».**

Le Président

Guy MAGNAN