GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Mesure du 8 février 2024 [9991064].

VOIR AUSSI la lettre d'information du 7 mars 2024

[doc. web n° 9991064].

Mesure du 8 février 2024

Registre des mesures
N° 66 du 8 février 2024

LE GARANT DE LA PROTECTION DES DONNÉES PERSONNELLES

Pasquale Stanzione, président, Ginevra Cerrina Feroni, vice-présidente, Guido Scorza et Agostino Ghiglia, membres, et Claudio Filippi, secrétaire général adjoint ;

VU le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (ci-après dénommé "le règlement") ;

VU le Code de protection des données personnelles, contenant des dispositions pour l'adaptation du système national au règlement (UE) 2016/679 (décret législatif n° 196 du 30 juin 2003, tel que modifié par le décret législatif n° 101 du 10 août 2018, ci-après "Code") ;

VU la violation de données à caractère personnel notifiée à l'Autorité le 22 octobre 2018, conformément à l'article 33 du règlement, par UniCredit S.p.a., relative à une attaque informatique sur le système de banque en ligne pour le canal web mobile ;

VU que, dans le cadre de l'enquête menée contre UniCredit S.p.a., des profils de responsabilité sont apparus à l'encontre de NTT Data Italia S.p.a., le responsable du traitement des données ;

A EXAMINÉ les pièces du dossier

AYANT PRIS CONNAISSANCE des observations formulées par le Secrétaire général adjoint conformément à l'article 15 du Règlement de la Garante n° 1/2000 ;

Dr Agostino Ghiglia ;

CONSIDÉRANT

1. La violation de données personnelles et l'activité d'investigation.

1.1. L'enquête contre UniCredit S.p.a.

Le 22 octobre 2018, UniCredit S.p.a. (ci-après " UniCredit " ou " la Banque ") a notifié au Garante, conformément à l'article 33 du règlement, la violation de données à caractère personnel survenue à la suite d'une attaque informatique sur le système de banque en ligne pour le canal web mobile

(ci-après " Mobile Banking Portal ") qui a entraîné l'acquisition illicite de certaines données à caractère personnel de clients (en particulier, le prénom, le nom, le code fiscal et le code d'identification interne de la banque, avec

l'exclusion de leurs données bancaires).

En particulier, la banque a représenté que les premières tentatives d'accès indu ont été effectuées dans la période comprise entre le 11 et le 20 octobre 2018 et que la cyberattaque s'est massivement réalisée le 21 octobre 2018, date à laquelle la banque, ayant détecté un grand nombre de tentatives de connexion vers le site de banque mobile, a immédiatement fourni la notification visée à l'article 33 du règlement, en précisant que :

> L'attaque a été réalisée par l'utilisation massive de codes séquentiels afin d'identifier ceux qui correspondent à des codes REB (code d'identification personnel pour l'accès au système bancaire en ligne) existants ;
>
> la violation a affecté "731.519 codes REB, dont [...] 6.859 étaient ceux bloqués par la banque parce que le mot de passe avait été identifié" ;
>
> Certaines données personnelles des clients (uniquement le nom, le prénom, le code fiscal et le code d'identification bancaire) étaient visibles dans le code de réponse à la requête, mais il ne semble pas qu'il y ait eu accès aux données bancaires des clients ou que des transactions aient été effectuées.

Dans une note ultérieure datée du 16 novembre 2018, la Banque, en réponse à une demande d'information formulée par l'Office le 9 novembre 2018, a également précisé que :

> L'attaque, provenant d'un réseau anonyme (TOR) et visant à masquer l'adresse IP réelle de l'attaquant, avait pour but d'énumérer un certain nombre de clients à l'aide d'un mot de passe fixe ;
>
> "une condition d'application permettait de renvoyer des informations même en cas d'échec de l'authentification et, par conséquent, lorsque le code REB saisi correspondait à un client, même si le mot de passe était correct, le nom et le prénom, le code fiscal et le NDG, qui est un code d'identification interne, attribué à chaque client au moment où il est saisi dans les systèmes informatiques [...] [d'UniCredit S.p.a.], ont été renvoyés. Pour les 6 859 clients qui avaient un mot de passe "faible" utilisé par les attaquants [...], le mot de passe a également été identifié" ;
>
> la réponse technologique immédiate, qui a eu lieu suite à l'identification ayant donné lieu à l'incident de sécurité, a consisté à bloquer les connexions individuelles provenant d'un réseau anonymisé (TOR) et présentant les caractéristiques d'une attaque informatique" ; en outre, "un blocage quantitatif des connexions dépassant un seuil critique par intervalle de temps défini et un mécanisme informatique (captcha) visant à l'identification humaine de l'utilisateur faisant la demande de connexion, dans le but de bloquer les connexions automatiques ou les scripts informatiques" ont également été mis en œuvre. [...] un mécanisme est en cours d'implémentation pour forcer l'utilisation de mots de passe complexes par les utilisateurs, qui sera disponible en production dès le 23 novembre et couvrira l'ensemble de la clientèle de la banque avec les versions ultérieures" ;
>
> En l'espèce, la banque, "ne considérant pas le "risque élevé" visé à l'article 34 du règlement et compte tenu du grand nombre de personnes concernées, a publié un avis sur son site web" et "a plutôt averti les clients dont les mots de passe devaient être bloqués parce qu'ils avaient été identifiés par les attaquants, et qui étaient au nombre de 6 859".

À la lumière d'un examen global des circonstances présentées par la banque, l'Autorité a considéré que la violation de données à caractère personnel en question, contrairement à l'évaluation faite par la banque, était susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques (condition pour laquelle la divulgation aux personnes concernées est requise) et que, par conséquent, avec l'aide de l'Autorité, la violation de données à

caractère personnel était susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques (condition pour laquelle la divulgation aux personnes concernées est requise).

mesure n° 499 du 13 décembre 2018 (doc. web n° 9076378) a enjoint à UniCredit, conformément à l'article 58, paragraphe 2, point e), du règlement, de communiquer la violation de données à caractère personnel à toutes les personnes concernées qui n'avaient pas déjà été destinataires d'une telle communication, en l'invitant à fournir une réponse dûment motivée sur les initiatives prises à cette fin ainsi que sur les mesures adoptées pour atténuer les effets négatifs de la violation de données à caractère personnel sur les personnes concernées.

Dans une note datée du 25 janvier 2019, la Banque, en décrivant les modalités et le calendrier avec lesquels elle a pris des mesures pour mettre en œuvre les exigences énoncées dans l'ordonnance n° 499 précitée, a précisé qu'elle avait préparé des avis différenciés pour les clients et les anciens clients (dont une copie est jointe en annexe), dont le contenu a été jugé conforme aux dispositions de l'article 34, paragraphe 2, du règlement.

Dans la même note, UniCredit a également annoncé que, suite à une analyse complémentaire menée afin d'identifier les personnes concernées devant être notifiées de la violation, il est apparu que le nombre de personnes concernées était plus élevé qu'initialement identifié (pour un nombre total de 777 765 clients et anciens clients) ; la banque a également précisé qu'elle avait mis en place un mécanisme de renforcement des mots de passe utilisés par les utilisateurs, initialement dirigé vers les clients concernés par la violation de données personnelles et progressivement étendu à l'ensemble de la base de clients d'ici mars 2019.

À l'issue d'enquêtes approfondies ultérieures (voir les demandes d'informations datées du 1er février et du 12 avril 2019), la Banque a fourni d'autres éléments de clarification (voir les notes datées du 26 février et du 3 mai 2019) sur la base desquels, également à la lumière de la documentation acquise au dossier, il est apparu que :

a) au moment de la violation de données à caractère personnel, en ce qui concerne la sécurité du traitement au sein du portail de banque mobile, les mesures techniques et organisationnelles visées à l'article 32 du règlement étaient les suivantes :

"login protégé par un nom d'utilisateur et un mot de passe remis séparément au client

dans l'agence ; compte bloqué après la saisie de trois mots de passe incorrects ;

le blocage des informations d'identification identifiées dans les fuites de données en ligne par [...] les services de renseignement/anti-fraude ;

possibilité pour le client de s'abonner à un service de messages textuels (SMS premium) l'informant d'activités telles que l'accès en ligne, le Pin et les modifications de données personnelles effectuées par la Banque via Internet ;

la protection des transactions et des activités sensibles (par exemple, la modification de données personnelles) en demandant un mot de passe à usage unique (OTP) supplémentaire ;

l'analyse comportementale et la surveillance des transactions pour détecter les fraudes au détriment des clients ;

effectuer des VA/PT périodiques [...] sur l'infrastructure et l'application Internet/bancaire ;

un pare-feu d'application web (WAF) pour se protéger contre les attaques web (par exemple, l'injection sql)" (voir note du 26 février 2019, pp. 1-2) ;

b) pendant la période " entre le 1er octobre 2018 et le 22 octobre 2018, un test de pénétration a été effectué sur le système Mobile Site (site et APP pour les appareils mobiles) ", dont l'exécution avait été confiée à la société NTT Data Italia S.P.A. (" NTT Data " ou " la société ") sur la base d'un accord conclu le 5 juin 2017 avec UniCredit Business Integrated.

Solutions S.c.p.a. (aujourd'hui UniCredit Services S.c.p.a., ci-après dénommée "UBIS") pour la fourniture de services de "tests de pénétration d'applications bancaires et d'évaluation de la vulnérabilité". Dans le cadre de cet accord, NTT Data avait été désignée par UniCredit comme responsable du traitement des données - conformément à l'article 29 du code en vigueur à l'époque - et avait reçu des instructions précises de la part d'UniCredit, notamment :

l'interdiction expresse de confier à des tiers l'exécution partielle ou totale des activités d'évaluation de la vulnérabilité et de tests de pénétration (voir section 14 de l'accord) ;

lorsque, pour l'exercice de certaines activités, il est nécessaire de recourir à un tiers, l'obligation d'informer le responsable du traitement afin que ce dernier puisse, après avoir évalué l'expérience, les compétences et la fiabilité du responsable du traitement, le désigner comme responsable du traitement ;

l'obligation, en cas de détection de vulnérabilités d'un niveau de gravité critique ou élevé, d'en informer immédiatement le titulaire afin de lui permettre de supprimer rapidement ces vulnérabilités (voir l'annexe 3 de l'accord) ;

c) NTT Data, dans le cadre de l'exécution des activités susmentionnées, a jugé nécessaire de se prévaloir de la collaboration d'une autre entité, Truel IT S.r.l. (ci-après " Truel IT "), qui, par acte de nomination en date du 17 septembre 2018, a été désignée comme sous-traitant secondaire en l'absence d'autorisation écrite préalable de la part d'UniCredit ;

d) le 19 octobre 2018, NTT Data a pris connaissance de deux vulnérabilités d'un niveau de gravité élevé (" Divulgation de données utilisateur " et " Absence de protection contre la force brute inversée ") par l'intermédiaire de Truel IT - qui lui a transmis le projet de rapport contenant les résultats des activités d'évaluation de la vulnérabilité et de test de pénétration - et n'en a informé UniCredit que le 22 octobre 2018.

1.2. L'enquête contre NTT Data Italia S.p.a.

Dans une note datée du 15 mai 2019, l'Autorité a adressé une demande d'informations à NTT Data qui, dans des communications datées des 24 et 27 mai 2019, a précisé que " les activités de test de pénétration et d'évaluation de la vulnérabilité ont été menées du 1er au 26 octobre 2018 selon le calendrier suivant " :

l'exécution des tests [...] a eu lieu du 1er au 12 octobre 2018 ;

l'analyse des résultats, la suppression des faux positifs, l'évaluation et la classification des vulnérabilités, la rédaction du rapport technique et l'envoi de ce même rapport en version provisoire au client du 13 au 22 octobre 2018 ;

des améliorations supplémentaires au document technique sur les vulnérabilités détectées du 22 au 26 octobre 2018, le rapport final ayant été envoyé au client le 26 octobre 2018".

NTT Data a également fourni des copies de rapports techniques contenant les résultats des activités d'évaluation des vulnérabilités et de tests de pénétration susmentionnées (en version préliminaire et finale), dans lesquels dix vulnérabilités détectées par Truel IT, dont deux vulnérabilités d'un niveau de gravité élevé, sont illustrées :

La première vulnérabilité de type "User Data Disclosure" a permis d'énumérer tous les identifiants d'utilisateur valides (composés de 8 chiffres après la virgule) pour l'accès au portail de banque mobile, et de saisir certaines données personnelles (telles que le prénom, le nom de famille et le code fiscal) associées à ces identifiants d'utilisateur, même sans connaître le code PIN correspondant (composé de 8 chiffres après la virgule) ;

la seconde vulnérabilité de type "manque de protection contre la force inverse" permettait un nombre illimité de tentatives d'authentification sur le portail de banque mobile avec des ID utilisateurs changeant constamment, sans être bloquées ; dans un tel scénario, un attaquant pouvait tenter d'identifier des paires ID utilisateur/NIP valides, par exemple en essayant des NIP particulièrement "faibles" tels que "00000000" ou "12345678".

NTT Data a par ailleurs indiqué avoir " pris connaissance de la vulnérabilité "User Data disclosure" le 19 octobre 2018 avec la remise du projet de rapport de Truel IT S.r.l." qui, pour sa part, avait identifié les deux vulnérabilités décrites ci-dessus respectivement le 10 octobre 2018 (la première) et le lendemain (la seconde) ; dans la même note, NTT Data a également souligné que "typiquement, les vulnérabilités potentielles d'un système sont détectées lors des activités de test de pénétration" et que "cette détection, cependant, nécessite, aux fins d'une évaluation des risques de la même et, par conséquent, d'une communication en temps opportun au client, l'exécution d'une activité d'analyse supplémentaire (élimination des faux positifs) et la classification (élevée, moyenne et faible) et la remédiation suggérée". Pour cette raison, elle a effectué, "conformément à la pratique, sa propre analyse des données reçues et une évaluation supplémentaire des classifications des 10 vulnérabilités détectées" et, seulement après conclusion, a notifié UniCredit "le 22 octobre 2018 à 10h00 CEST".

Enfin, NTT Data a précisé que "la détection [...] des vulnérabilités en question ne pouvait pas déterminer et n'a pas déterminé la connaissance/détection par NTT DATA Italia de la violation des données personnelles".

2. L'ouverture d'une procédure pour l'adoption de mesures correctives et de sanctions et les observations de NTT Data Italia S.p.a..

À l'issue des enquêtes décrites ci-dessus, caractérisées par un niveau élevé de complexité des profils technologiques (voir le rapport technique du 10 décembre 2019), l'Office a mis en évidence les problèmes critiques rencontrés en ce qui concerne le respect par le responsable du traitement et le sous-traitant de leurs obligations en matière de protection des données.

En particulier, l'analyse de la documentation acquise dans le dossier et des déclarations faites par NTT Data, le responsable du traitement des données d'UniCredit (dont la responsabilité est engagée en vertu de l'article 168 du Code, "Fausses déclarations au Garante et interruption de l'exercice des fonctions ou des pouvoirs du Garante"), a permis de constater ce qui suit

NTT Data a confié la réalisation de l'évaluation de la vulnérabilité et des tests de pénétration du portail bancaire mobile en question à une société tierce (Truel IT) sans autorisation écrite préalable du responsable du traitement, en violation de l'article 28, paragraphe 2, du règlement ;

NTT Data a informé tardivement UniCredit de la violation de données à caractère personnel et n'a donc pas respecté son obligation au titre de l'article 33, paragraphe 2, du règlement.

Compte tenu de ce qui précède, l'Office, par note en date du 5 février 2020, a notifié à NTT Data Italia S.p.A, responsable du traitement des données d'UniCredit, l'ouverture de la procédure d'adoption des mesures visées à l'article 58, paragraphe 2, et à l'article 83 du règlement, conformément aux dispositions de l'article 166, paragraphe 5, du code, en ce qui concerne la violation alléguée des dispositions régissant le recours à un autre responsable du traitement des données et de l'obligation d'informer le responsable du traitement des données en cas de violation de données à caractère personnel visée à l'article 28, paragraphe 2, et à l'article 33, paragraphe 2, du règlement.

Dans la même note, NTT Data a été invitée à produire des écrits ou des documents défensifs ou à demander à être entendue par l'Autorité (article 166, paragraphes 6 et 7, du code et article 18,

paragraphe 6, du code).

1, loi n° 689 du 24 novembre 1981).

Le 20 mars 2020, NTT Data Italia a présenté son mémoire en défense, qui est rappelé ici dans son intégralité, dans lequel, en formulant sa demande d'audition, elle a fourni les éléments d'appréciation suivants (avec la documentation jointe). En particulier :

a) " les activités VA et PT qui font l'objet de la vérification de ce jour par le Garant ont été réalisées par NTT Data, pour le compte d'UBIS (et non d'UniCredit), dans la période du 1er octobre 2018 au 12 octobre 2018, en exécution du contrat du 5 juin 2017 relatif à " Banking Application Penetration Test & Vulnerability Assessment " et, en vertu duquel, un bon de commande spécifique a été émis par UBIS à l'attention de NTT Data ". Donc " C'est UBIS, et seulement UBIS, la société du groupe UniCredit avec laquelle NTT Data avait des relations contractuelles ". En effet :

le contrat a été signé par UBIS et NTT Data ;

la dernière désignation de NTT Data en tant que sous-traitant ou soustraitant (et non responsable de traitement) pour le traitement a été faite par UBIS, en sa qualité de sous-traitant ou de responsable de traitement, le 18 octobre 2018 (Data Processing Agreement ou DPA) ;

il est expressément prévu que les obligations du RGPD prévalent, en cas de conflit, sur celles du Contrat (art. 12.1. du RGPD), avec pour conséquence que, à compter du 18 octobre 2018, la désignation de NTT Data en tant que processeur de données pour UniCredit en vertu de l'art. 13 du Contrat est réputée annulée et remplacée par le RGPD ;

L'UBIS (et non UniCredit) apparaît dans la DPA comme la seule entité devant être notifiée de toute violation de données ou de données à caractère personnel (voir l'annexe 1 de la DPA - p. 8) ;

les lettres d'autorisation spécifique pour l'exercice des activités de VA et de PT sur les systèmes bancaires mobiles d'UniCredit (Android et iOS) soumis à la vérification de la Garante ont été signées par UBIS [...].

Sans préjudice de ce qui précède, il est également vrai que l'annexe 1 du contrat [...] prévoit que NTT Data doit effectuer des activités de VA et de PT sur les systèmes de différentes sociétés du groupe UniCredit : mais il est tout aussi vrai que ces activités seraient, et ont toujours été, effectuées pour le compte d'UBIS, et non d'UniCredit" ;

b) "NTT Data n'avait aucune obligation envers UniCredit : toutes ses obligations étaient envers l'UBIS, avec pour conséquence qu'aucun retard dans la communication de quoi que ce soit à UniCredit ne peut lui être imputé. Quant aux obligations assumées par NTT Data en vertu du contrat et de la DPA, celles qui sont pertinentes pour la présente procédure sont citées :

réaliser, pour le compte de l'UBIS, des activités de VA et de PT (articles 3.1. et 3.2. du Contrat) ;

notifier immédiatement à l'UBIS toute vulnérabilité critique ou de haut niveau (voir p. 4 de l'annexe 3 du contrat) ;

notifier à l'UBIS, dans les meilleurs délais, toute violation de données à caractère personnel (article 6.1. du RGPD) ;

notifier à l'UBIS immédiatement et, en tout état de cause, dans un délai de 4 heures après en avoir pris connaissance, toute violation de données à caractère personnel

(article 6.2. du RGPD) ;

demander l'autorisation préalable de l'UBIS pour l'engagement de tout sous-traitant supplémentaire (article 9.1. du RGPD)" ;

c) "La raison pour laquelle l'intervention de Truel It a été nécessaire est la même que celle pour laquelle UBIS n'a pas obtenu d'autorisation préalable : faire face à un pic de travail soudain et inattendu. L'intervention de Truel It s'est toutefois limitée à un seul cas, celui de l'exécution de VA et PT que la Garante examine aujourd'hui. Le pic de travail signalé n'était toutefois pas de nature à porter préjudice à la position d'UBIS ou des personnes concernées [...]. En effet, Truel It n'est intervenue qu'en tant que fournisseur inscrit a u registre de NTT Data, c'est-à-dire parce que son professionnalisme et sa fiabilité avaient déjà été vérifiés par la collecte des documents et des autocertifications/autodéclarations nécessaires, y compris celle concernant les mesures de sécurité organisationnelles et techniques mises en œuvre" ;

d) " la réalisation des activités VA et PT entre le 1er octobre 2018 et le 12 octobre 2018 a eu lieu en exécution d'une demande spécifique de l'UBIS. Les vérifications effectuées par NTT Data (également via Truel It) ont consisté, spécifiquement, à simuler des scénarios d'intrusion vers l'application cible afin de vérifier sa résistance à des actions potentielles visant à créer des conditions de disservice et/ou de vol de données/informations critiques (ce que l'on appelle l'exfiltration de données). Toutes ces activités ont été constamment surveillées par l'UBIS par l'intermédiaire de son centre opérationnel de sécurité. Le périmètre d'intervention convenu avec l'UBIS, la nature même des activités confiées à NTT Data par l'UBIS et les outils utilisés par le personnel de NTT Data et de Truel It dans le cadre de ces activités ne permettaient pas - ni n'auraient pu permettre - de détecter les tentatives d'intrusion (réelles et non simulées) menées par des tiers. En particulier, la détection d'une tentative d'accès par un tiers aux systèmes d'UBIS peut se faire au moyen de [...]" une série d'activités "non comprises dans la mission confiée à NTT Data (et, par conséquent, à Truel It) [...] les seules [...] qui auraient permis la détection de tentatives d'accès aux systèmes d'UBIS. [...]. NTT Data, toujours par l'intermédiaire de Truel It, s'est limitée aux activités nécessaires à l'accomplissement de la mission qu'elle avait reçue : l'exécution de VA et de PT. Dans ce contexte, Truel It a produit (le 19 octobre 2018) un rapport intermédiaire, que NTT Data a vérifié selon ses pratiques internes, à titre d'assurance qualité. "

e) En ce qui concerne spécifiquement les objections soulevées par l'Autorité, la société a tout d'abord souligné deux circonstances : la première est que 'NTT Data n'avait aucune relation ni aucune obligation envers UniCredit : il ne semble donc pas possible de contester qu'elle ait communiqué quoi que ce soit à UniCredit avec retard ; la seconde est que 'NTT Data n'a pas eu la possibilité de détecter (au nom d'UBIS) les tentatives d'accès aux systèmes d'UniCredit, qui ont abouti à la violation de données notifiée par cette dernière au Garant. La tâche qu'elle a accomplie (également avec Truel It) concernait un tout autre domaine, à savoir l'évaluation de la vulnérabilité et les tests de pénétration et, dans ce contexte, elle n'avait pas accès aux outils qui auraient pu lui permettre de détecter (pour le compte de l'UBIS) les tentatives d'accès non autorisé aux systèmes d'UniCredit". Cela dit, il convient de souligner que :

1. "en ce qui concerne la violation de l'article 28, paragraphe 2, du règlement :

   la même chose s'est produite dans la " période de première application du GDPR, 8 mois à compter du 19 septembre 2018 au 19 mai 2019 ", période dont - conformément à " l'article 22, paragraphe 13 du décret législatif 101/2018 - le Garant [...] tient compte, aux fins de l'application des sanctions administratives et dans la mesure compatible avec les dispositions du règlement [...] ". Par conséquent, "le fait que NTT Data, de bonne foi, par négligence excusable (et certainement pas par malveillance ou négligence grave), n'a pas demandé l'autorisation préalable d'UBIS pour engager Truel It doit donc être évalué sous cet angle [...]" :

   ni l'UBIS, ni les parties intéressées n'ont subi de préjudice du fait de l'implication de Truel It dans l'exécution de VA et PT" ; celles-ci "ont été exécutées (non pas par NTT Data, mais) par Truel It, mais toujours dans les règles de l'art et conformément aux

spécifications convenues par contrat avec

UBIS [...] En substance, si NTT Data avait exercé directement les activités de VA et de PT, elle les aurait exercées de la même manière que Truel It [...]" ; par conséquent, "[...] à cet égard également, l'omission de NTT Data apparaît comme une simple légèreté, en tant que telle dépourvue (à tous égards) du caractère offensant" ;

"La manière dont Truel It a exécuté la VA et la PT, telle que décrite dans le rapport remis par Truel It à NTT Data, signifie qu'une grande partie des tests demandés par UBIS ont été effectués sur des comptes courants de référence et de test, ce qui a exclu toute interaction massive (par NTT Data et/ou Truel It) avec d'autres comptes courants associés à des clients réels, avec pour résultat que l'intégrité et la confidentialité des données de ces derniers ont été préservées. En particulier, l'Autorité, en décidant d'imposer ou non une sanction, devrait également tenir compte du fait que, dans l'exécution de la VA et de la PT, Truel It a pris connaissance, pendant une période de temps extrêmement limitée (1-12 octobre 2018), de simples données d'identification (prénom, nom et code fiscal) et que celles-ci, "en application des principes de minimisation, de finalité et de limitation du stockage, lorsqu'elles ont été affichées par les systèmes d'UniCredit à l'issue de la requête - ont été promptement supprimées des systèmes de Truel It" ;

NTT Data " n'a encore jamais fait l'objet d'inspections et/ou de sanctions de la part de l'Autorité ; il s'agit sans aucun doute d'une indication claire du bon (voire même de l'excellent) niveau de conformité atteint par l'entreprise [...]", comme en témoignent les différentes " mesures de conformité déjà en place au 22 octobre 2018 " et celles adoptées après le 22 octobre 2018 et actuellement en cours de mise en œuvre (dont une description complète a été fournie en annexe du mémoire en défense). "Pour confirmer et conforter ce qui précède, il faut également considérer que NTT Data, agissant souvent en tant que (sous-)responsable de traitement, est tout aussi souvent soumis à des audits par ses clients (responsables de traitement ou sous-traitants de données) : ces audits sont toujours couronnés de succès."

"une éventuelle sanction pour violation de l'article 28, paragraphe 2, du RGPD (une disposition régissant la relation entre le responsable du traitement et le propriétaire et, par conséquent, entre NTT Data et ses clients)" entraînerait une atteinte à la réputation (c'est-à-dire "la perte de la confiance des clients et, par conséquent, la perte de commissions") "d'une gravité franchement disproportionnée par rapport à la légèreté de la violation contestée" ;

2. en ce qui concerne la violation alléguée de l'article 33, paragraphe 2, du règlement, il est à nouveau réitéré que "NTT Data n'avait pas, et n'aurait pas pu avoir, connaissance de la violation de données à caractère personnel subie par UniCredit le 21 octobre 2018", et ce pour les raisons suivantes :

"La mission de NTT Data consistait à effectuer des évaluations de vulnérabilité et des tests de pénétration, rien d'autre ;

le plaignant d'aujourd'hui n'était notamment pas responsable de la surveillance des systèmes informatiques d'UniCredit : il n'avait donc aucun moyen de détecter les attaques et/ou les violations de données (circonstance également confirmée par le rapport technique : voir p. 5 et s.)

En outre, l'accès aux systèmes d'UniCredit s'est arrêté le 12 octobre 2018, lorsque Truel.it a conclu ses activités et a commencé à rédiger le rapport d'évaluation de la vulnérabilité et de test de pénétration : bien avant, donc, que la violation de données du 21 octobre 2018 ne se produise".

La société a ensuite de nouveau souligné que "la seule chose que NTT Data aurait pu détecter, et

qu'elle a détectée, était une vulnérabilité de haut niveau qu'elle a divulguée à UBIS en temps opportun au moment où elle en a eu connaissance. [...] NTT Data n'a pas

connaissait, et ne pouvait pas connaître, la violation de données d'UniCredit du 21 octobre 2018 : articles 6.1. et 6.2.
6.2. du RGPD n'ont donc pas été violées. La seule chose dont NTT Data a eu connaissance était la vulnérabilité exploitée par les tiers auxquels la violation de données subie par UniCredit est imputable : quelque chose de tout à fait différent de la violation de données elle-même. Et il n'est pas allégué que NTT Data a tardé à communiquer cette vulnérabilité : elle n'aurait pas pu le faire, car la vulnérabilité a été communiquée en temps utile.

Le Contrat, à cet égard, prévoyait que la communication [était] immédiate. La notion d'immédiateté est, bien entendu, soumise à la connaissance effective que NTT Data a pu avoir de la vulnérabilité : ce moment n'est pas antérieur au 19 mars 2018, c'est-à-dire le jour où NTT Data a reçu le rapport préliminaire de Truel It ([...] annexé au Rapport technique), et il n'est pas non plus fortuit. Le groupe de travail Article 29, dans ses lignes directrices sur la notification des violations de données à caractère personnel, a précisé que le délai pour une telle notification court à partir du moment où le responsable du traitement ou le sous-traitant (selon le cas) acquiert la connaissance effective de la violation elle-même, et que la connaissance effective suit nécessairement la diligence raisonnable. Ce principe est manifestement aussi applicable au cas de NTT Data, sur la base d'un principe de vraisemblance : si une circonstance grave telle qu'une violation de données doit être vérifiée avant d'être notifiée, on voit mal pourquoi une circonstance moins grave, telle qu'une vulnérabilité, devrait être notifiée avant qu'il ait été vérifié qu'elle est effective.

Aucun retard n'est donc imputable à NTT Data : ni en ce qui concerne la communication de la violation des données d'UniCredit, dont elle ne pouvait pas avoir connaissance, ni en ce qui concerne la vulnérabilité, qu'elle a communiquée dès qu'elle en a eu connaissance".

L'entreprise a ensuite souligné que, en résumé, il ressort des faits que

> NTT Data n'avait pas, et n'aurait pas pu avoir, connaissance de la violation de données (et des tentatives antérieures de tiers d'accéder aux systèmes) d'UniCredit ;
>
> NTT Data ne pouvait pas, et ne pouvait pas, communiquer la violation de données à UniCredit ;
>
> le seul fait dont NTT Data avait connaissance était une vulnérabilité des systèmes d'UniCredit [...] qui a été rapidement communiquée par NTT Data, puisque UBIS en a été informé dès que NTT Data a terminé s e s vérifications pour s'assurer que le rapport de Truel It était correct" ;
>
> même si NTT avait transmis le rapport de Truel IT "immédiatement, c'est-à-dire dès le 19 octobre 2018, sans attendre de le faire vérifier", UBIS n'aurait pas pu éviter la violation de données à caractère personnel "parce qu'il s'est écoulé très peu de temps entre le 19 octobre et le 21 octobre".

Le 19 janvier 2021, l'audition de NTT Data a eu lieu, au cours de laquelle NTT Data, tout en réitérant pleinement ce qu'elle avait déjà exposé dans son mémoire en défense, a demandé que l'Autorité, aux fins de l'évaluation de l'affaire, prenne particulièrement en considération les circonstances suivantes :

> a) aucun dommage n'est survenu du fait de l'activité exercée par l'entreprise" ;
>
> b) "les faits se sont produits au cours d'une période particulièrement difficile qui a entraîné la nécessité de recourir à un tiers, qui plus est à un stade de première application du GDPR" ;
>
> c) l'entreprise a coopéré avec l'Autorité, en fournissant tous les éléments utiles à la reconstitution de l'accident" ;

d) "l'application éventuelle d'une amende et surtout la publication de l'avis d'appel d'offres".

serait très préjudiciable aux intérêts de la société et réduirait à néant tous les efforts réalisés jusqu'à présent, en termes de conformité, lorsque cet aspect est un élément de concurrence entre les acteurs du secteur".

L'entreprise a également souligné qu'elle s'engageait à adopter d'autres mesures "afin de continuer à élever le niveau de conformité, dont certaines sont encore en cours de mise en œuvre (une phase qui devrait s'achever [...] d'ici au 31 mars 2021)". [...] entre autres, le tableau de bord de la protection de la vie privée, qui permet à l'entreprise (et, en particulier, à son service de protection de la vie privée) de (i) surveiller en permanence les aspects liés à la protection de la vie privée afin d'identifier les domaines à améliorer conformément au principe de responsabilité, et (ii) de préparer des rapports périodiques sur le niveau de conformité en matière de protection de la vie privée, qui seront communiqués à la direction générale".

3. Législation sur la protection des données personnelles.

Conformément à l'article 28, paragraphe 2, du règlement, "le responsable du traitement ne peut avoir recours à un autre responsable du traitement sans l'autorisation écrite, spécifique ou générale et préalable du responsable du traitement [...]".

Le paragraphe 3 du même article 28 du règlement, en prévoyant que "le traitement p a r un responsable du traitement est régi par un contrat ou un autre acte juridique", précise, au point f), que ce contrat ou cet autre acte juridique doit prévoir que le responsable du traitement "l'aide à assurer le respect des obligations visées aux articles 32 à 36, compte tenu de la nature du traitement et des informations dont dispose le responsable du traitement".

En outre, l'article 28, paragraphe 4, du règlement prévoit que "lorsqu'un responsable du traitement confie à un autre responsable du traitement le soin d'effectuer des activités de traitement spécifiques pour le compte du responsable du traitement [...]". L'article 28, paragraphe 4, du règlement prévoit que "lorsqu'un responsable du traitement confie à un autre responsable du traitement le soin d'effectuer des activités de traitement spécifiques pour le compte du responsable du traitement [....les mêmes obligations en matière de protection des données contenues dans le contrat ou dans tout autre acte juridique en vertu du droit de l'Union ou du droit des États membres sont imposées à cet autre responsable du traitement que celles contenues dans le contrat ou dans tout autre acte juridique entre le responsable du traitement et le responsable du traitement visé au paragraphe 3, en prévoyant notamment des garanties suffisantes pour mettre en œuvre les mesures techniques et organisationnelles appropriées afin de veiller à ce que le traitement réponde aux exigences du règlement [...]". Lorsque l'autre responsable du traitement manque à ses obligations en matière de protection des données, le responsable du traitement initial conserve, à l'égard du responsable du traitement, l'entière responsabilité du respect des obligations de l'autre responsable du traitement".

L'article 33, paragraphe 2, du règlement, relatif aux violations de données à caractère personnel, prévoit que, dans ce cas, "le responsable du traitement informe le responsable du traitement dans un délai raisonnable après avoir pris connaissance de la violation".

4. Les évaluations de l'Autorité et les résultats de l'enquête.

Après avoir examiné la documentation produite et les déclarations faites par le responsable du traitement au cours de la procédure, étant donné que, à moins que l'acte ne constitue un délit plus grave, quiconque, dans une procédure devant le Garante, déclare ou atteste faussement des informations ou des circonstances ou produit des actes ou des documents faux est responsable en vertu de l'article 168 du code, la présente Autorité formule les observations finales suivantes.

En ce qui concerne la violation contestée de l'article 28, paragraphe 2, du règlement, il convient de noter que NTT Data a confié à la société Truel IT la réalisation d'activités d'évaluation de la vulnérabilité et de tests de pénétration sans avoir obtenu l'autorisation écrite préalable nécessaire,

spécifique ou générale, du responsable du traitement des données.

En outre, le même acte désignant NTT Data comme responsable du traitement contenait les éléments suivants

l'interdiction expresse de confier à des tiers la réalisation partielle ou totale des activités d'évaluation de la vulnérabilité et de tests de pénétration.

En ce qui concerne le deuxième profil contesté, compte tenu de ce qui a été amplement démontré au cours de l'enquête par UniCredit et NTT Data, il apparaît que

a) les deux vulnérabilités susmentionnées, identifiées comme étant de "haute sévérité", sont exactement celles utilisées par l'attaquant lors de la cyberattaque qui a été menée, de manière massive, pour identifier les ID utilisateurs (codes REB) valables pour l'accès au portail Mobile Banking et pour acquérir de manière illicite les données personnelles qui leur sont associées ;

b) Truel IT était " consciente " de la violation de données à caractère personnel à partir du moment où elle a détecté la vulnérabilité de type " User Data Disclosure " (c'est-à-dire telle que reflétée dans les rapports techniques, à partir du 10 octobre 2018), car à ce moment-là, il y avait une certitude raisonnable qu'une violation de la confidentialité des données à caractère personnel traitées au sein du Mobile Banking Portal s'était produite. En outre, l'identification, par la même société, le jour suivant immédiatement (11 octobre 2018), de la vulnérabilité de type "Absence de protection contre la force brute inversée" a mis en évidence la circonstance que la vulnérabilité de type "Divulgation des données de l'utilisateur" pouvait être exploitée à grande échelle, produisant des effets négatifs sur un grand nombre de personnes concernées ;

c) Truel IT n'a informé NTT Data des vulnérabilités susmentionnées que le 19 octobre 2018, en lui envoyant le projet de rapport contenant les résultats des activités d'évaluation des vulnérabilités et de tests de pénétration, et ce n'est que le 22 octobre 2018, le lendemain de la cyberattaque, que NTT Data a informé UniCredit (alors que la Banque en avait déjà eu connaissance de manière indépendante, puisque ses systèmes de surveillance avaient détecté la cyberattaque du 21 octobre 2018 et avaient par conséquent adopté une première série de mesures techniques et organisationnelles pour remédier à la violation des données à caractère personnel).

Au vu de ce qui précède, notant tout d'abord que les activités confiées par la banque à NTT Data peuvent être assimilées à celles qu'un responsable du traitement effectue afin de "tester, vérifier et évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement" (voir l'article 32, paragraphe 1, point d), du règlement), il s'ensuit qu'en cas de violation de données à caractère personnel, bien que le responsable du traitement conserve la responsabilité générale de la protection des données à caractère personnel, il joue un rôle fondamental en permettant au responsable du traitement d'assurer la sécurité de ce dernier. (En vertu de l'article 28, paragraphe 3, point d), du règlement, il s'ensuit qu'en cas de violation de données à caractère personnel, bien que le responsable du traitement conserve la responsabilité générale de la protection des données à caractère personnel, il joue néanmoins un rôle essentiel pour permettre au responsable du traitement de s'acquitter en temps utile et de manière adéquate des obligations qui lui incombent en vertu des articles 32 à 36 du règlement (voir article 28, paragraphe 3, point f)), y compris celles relatives à la notification des violations de données à caractère personnel.

En particulier, en vertu de l'article 33, paragraphe 2, du règlement, en cas de violation de données à caractère personnel, le responsable du traitement est tenu d'informer "le responsable du traitement dans un délai raisonnable après avoir pris connaissance de la violation".

À cet égard, en ce qui concerne l'expression " sans retard injustifié ", les " Lignes directrices 9/2022 sur la notification des violations de données à caractère personnel en vertu du GDPR ", adoptées par le Comité européen de la protection des données le 28 mars 2023 (qui ont remplacé les précédentes " Lignes directrices sur la notification des violations de données à caractère personnel en vertu du règlement (UE) 2016/679 " adoptées par le groupe de travail Article 29 sur

la protection des données [...] en dernier lieu le 6 février 2018 et approuvées par le Comité européen de protection des données le 25 mai 2018), recommandent que le responsable du traitement des données "effectue la notification au responsable du traitement des données en temps utile, en fournissant par la suite toute information supplémentaire sur la violation dont il a connaissance" ; ceci est "important pour aider le responsable du traitement à respecter son obligation de notification à l'autorité de contrôle dans les 72 heures".

Il en va de même lorsque, comme en l'espèce, un responsable du traitement emploie un sous-traitant ultérieur pour effectuer des activités de traitement spécifiques pour le compte d'un responsable du traitement ; l'obligation d'informer le responsable du traitement prévue à l'article 33, paragraphe 2, reste à la charge du responsable du traitement initial, qui n'est pas tenu d'évaluer le risque découlant de la violation de données avant d'informer le responsable du traitement ; le responsable du traitement est uniquement tenu de déterminer si une violation de données à caractère personnel s'est produite et, dans l'affirmative, d'en informer le responsable du traitement. L'obligation d'informer le responsable du traitement prévue à l'article 33, paragraphe 2, reste à la charge du responsable du traitement initial, qui n'est pas tenu d'évaluer le risque découlant de la violation avant d'informer le responsable du traitement ; il appartient uniquement au responsable du traitement de déterminer si une violation de données à caractère personnel s'est produite et, dans l'affirmative, de l'informer sans délai ; il appartient au responsable du traitement de procéder à cette évaluation, une fois qu'il a pris connaissance de la violation.

En l'espèce, NTT Data aurait donc dû informer le responsable du traitement de la violation de données à caractère personnel sans délai, c'est-à-dire dès les 11 et 12 octobre 2018, lorsqu'elle en a eu connaissance par l'intermédiaire de Truel IT.

Il s'agit de permettre au titulaire de :

de prendre rapidement les mesures nécessaires pour supprimer les vulnérabilités susmentionnées, afin d'éviter qu'elles ne soient exploitées par un éventuel attaquant ;

vérifier si des vulnérabilités ont déjà été exploitées pour acquérir illicitement des données à caractère personnel et ainsi limiter la portée de la cyberattaque ;

respecter, le cas échéant, les obligations de notification à l'Autorité et d'information des personnes concernées prévues aux articles 33 et 34 du règlement.

Il convient également d'ajouter que le choix de la société d'externaliser les activités d'évaluation des vulnérabilités et de tests de pénétration a probablement contribué au retard dans la communication de la violation au propriétaire, circonstance qui a ensuite eu une incidence négative sur la rapidité des mesures correctives adoptées par le propriétaire lui-même pour supprimer les vulnérabilités susmentionnées.

5. Conclusion : déclaration de traitement illicite. Mesures correctives en vertu de l'article 58, paragraphe 2, du règlement.

Pour les raisons susmentionnées, l'Autorité considère que les déclarations faites par NTT Data dans les mémoires en défense - dont la véracité peut être mise en cause en vertu de l'article 168 du code susmentionné - bien qu'elles méritent d'être prises en considération, ne permettent pas de surmonter les conclusions notifiées par l'Office avec l'acte d'ouverture et sont insuffisantes pour permettre le rejet de la procédure, étant donné qu'aucun des cas prévus par l'article 11 du règlement n° 1/2019 du Garante, concernant les procédures internes de l'Autorité ayant une pertinence externe, n'est applicable.

En particulier, à la lumière des considérations exposées au point 4, il est déclaré que NTT Data, en ce qui concerne la violation de données à caractère personnel en question - indépendamment des considérations sur les profils de responsabilité d'UniCredit S.p.a. en tant que responsable du traitement, qui font l'objet d'une mesure séparée et distincte - a adopté un comportement illicite en violation de l'article 28, paragraphe 2, et de l'article 33, paragraphe 2, du règlement.

Par conséquent, compte tenu de la nature des infractions, l'Autorité, dans l'exercice des pouvoirs de correction conférés par l'article 58, paragraphe 2, du règlement, estime qu'il n'est pas nécessaire d'ordonner des mesures correctives au titre de l'article 58, paragraphe 2, point d), et

ordonne une sanction administrative pécuniaire au titre de l'article 83 du règlement, proportionnée aux circonstances de l'espèce (article 58, paragraphe 2, point i)).

6. Ordonnance d'injonction.

La violation des dispositions susmentionnées entraîne l'application de la sanction administrative prévue à l'article 83, paragraphe 4, point a), du règlement.

En ce qui concerne les éléments énumérés à l'article 83, paragraphe 2, du règlement aux fins de l'application de la sanction administrative pécuniaire et de sa quantification, compte tenu du fait que la sanction doit être "dans tous les cas effective, proportionnée et dissuasive" (article 83, paragraphe 1, du règlement), il est indiqué que, dans le cas présent, les circonstances suivantes ont été prises en considération :

a) en ce qui concerne la nature, la gravité et la durée des violations (article 83, paragraphe 2, point a), du règlement), la circonstance que l'entreprise n'a eu connaissance des violations qu'après que les données à caractère personnel ont fait l'objet d'une violation et que le responsable du traitement des données a demandé des éléments a été jugée pertinente ;

b) en ce qui concerne le caractère délibéré ou négligent des violations et le degré de responsabilité du responsable du traitement (article 83, paragraphe 2, points b) et d), du règlement), il a été tenu compte du comportement négligent de l'entreprise en tant que responsable du traitement, qui n'a pas respecté les règles relatives à la protection des données à caractère personnel, tant en ce qui concerne les obligations incombant au responsable du traitement (article 28, paragraphe 2, et 33, paragraphe 2, du règlement) que par rapport aux instructions légitimes du responsable du traitement (interdiction de confier à des tiers l'exécution partielle ou totale des activités d'évaluation de la vulnérabilité et de tests de pénétration) ;

c) l'absence de mesures antérieures de l'Autorité à l'encontre de l'entreprise (article 83, paragraphe 2, point e), du règlement) ;

d) une coopération efficace avec l'Autorité, y compris en ce qui concerne la reconstitution des événements et les relations avec le responsable du traitement (article 83, paragraphe 2, point f), du règlement) ;

e) en ce qui concerne les catégories de données à caractère personnel concernées par la violation (article 83, paragraphe 2, point g), du règlement), les données concernées par la violation étaient des données communes aux personnes concernées.

En considération des principes d'efficacité, de proportionnalité et de dissuasion susmentionnés (article 83, paragraphe 1, du règlement), que l'Autorité doit suivre pour déterminer le montant de la sanction, les conditions économiques du contrevenant ont été prises en considération, déterminées sur la base des recettes réalisées en référence aux états financiers pour l'année 2022.

Sur la base des éléments ci-dessus, appréciés globalement, il y a lieu de déterminer le montant de l'amende à hauteur de 800 000 (huit cent mille) euros pour la violation des articles 28, paragraphe 2, et 33, paragraphe 2, du règlement.

Dans ce contexte, et compte tenu du type de violation constatée, il est considéré que, conformément à l'article 166, paragraphe 7, du Code et à l'article 16, paragraphe 1, du Règlement du Garant n° 1/2019, cette disposition doit être publiée sur le site Internet du Garant.

Enfin, il convient de noter que les conditions préalables énoncées à l'article 17 du règlement n° 1/2019 concernant les procédures internes ayant une pertinence externe, visant à l'accomplissement des tâches et à l'exercice des pouvoirs confiés à la Garante, sont remplies.

TOUT CE QUI PRÉCÈDE, LE SUPERVISEUR

Déclare, en vertu des articles 57, paragraphe 1, point f), et 83 du règlement, que le traitement effectué est illicite, dans les termes prévus dans les motifs, pour violation des articles 28, paragraphe 2, et 33, paragraphe 2, du règlement.

COMMANDE

à NTT Data Italia S.p.a., dont le siège est à Milan, Via Ernesto Calindri, 4, C.F./P.I. 00513990010, en vertu de l'article 58, paragraphe 2, lettre i), du règlement, de payer la somme de 800 000 (huit cent mille) euros à titre d'amende administrative pour les violations indiquées dans la présente mesure ;

INGIUNGE

à la même NTT Data Italia S.p.a. de verser la somme de 800 000 (huit cent mille) euros selon les modalités précisées en annexe, dans un délai de 30 jours à compter de la notification de la présente mesure, sous peine d'adoption des mesures d'exécution qui en découlent, conformément à l'article 27 de la loi n° 689/1981.

Il convient de noter qu'en vertu de l'article 166, paragraphe 8, du Code, le droit du contrevenant de régler le litige en payant - toujours selon les termes énoncés dans l'annexe - un montant égal à la moitié de la sanction imposée dans le délai prévu à l'article 10, paragraphe 3, du décret législatif n° 150 du 1er septembre 2011 pour l'introduction du recours, comme indiqué ci-dessous, reste inchangé.

FOURNIT

Conformément à la Section 166(7) du Code et à la Section 16(1) du Règlement n° 1/2019 du Garant, la publication de cette ordonnance sur le site Internet du Garant et considère que les exigences de la Section 17 du Règlement n° 1/2019 sont satisfaites.

Conformément à l'article 78 du règlement, ainsi qu'à l'article 152 du code et à l'article 10 du décret législatif n° 150 du 1er septembre 2011, un recours contre cette mesure peut être introduit devant les autorités judiciaires ordinaires, à peine d'irrecevabilité, dans un délai de trente jours à compter de la date de communication de la mesure elle-même, ou dans un délai de soixante jours si le requérant réside à l'étranger.

Rome, 8 février 2024

LE PRÉSIDENT
Stanzione

L'INTERVENANT
Ghiglia

LE SECRÉTAIRE GÉNÉRAL ADJOINT
Filippi