Avis de contrôle préalable

«Le traitement de données dans le cadre de la veille sur les réseaux sociaux» à la Banque centrale européenne (BCE)

Dossier 2017-1052

***

La BCE envisage de s'adjoindre les services d'un prestataire externe qui sera chargé d'assurer une surveillance et un suivi des commentaires publiés sur des sujets relatifs à la BCE sur différents réseaux sociaux. Le traitement a pour finalité de voir comment les internautes parlent de la BCE sur les réseaux sociaux (par exemple, après des conférences de presse, des discours, des entretiens, des décisions de politique monétaire, des auditions du Parlement européen et d'autres événements) et d'améliorer la communication et la réputation de la BCE. À cette fin, la BCE souhaite collecter des informations sur les propos qui sont tenus à son égard ou sur des sujets la concernant, sur le ton employé et sur la mesure dans laquelle ces informations sont diffusées. Le prestataire externe procédera au suivi et à l'analyse des données agrégées concernant différents groupes d'utilisateurs. La BCE analysera ces informations et établira des rapports. Certains internautes, qui ne sont pas des personnes publiques, peuvent être indirectement identifiables à partir de leurs commentaires, de leurs appréciations ou de leur langue maternelle.

***

Bruxelles, le 21 mars 2018

Adresse postale: rue Wiertz 60 – B-1047 Bruxelles
Bureaux: rue Montoyer 30 – B-1000 Bruxelles
Courriel: edps@edps.eu.int Site internet: http://www.edps.europa.eu
Tél. 32 2-283 19 00 – Fax 32 2-283 19 50

1. Procédure

Le 29 novembre 2017, le contrôleur européen de la protection des données (ci-après le «CEPD») a reçu du délégué à la protection des données (ci-après le «DPD») de la BCE une notification de contrôle préalable au titre de l'article 27, paragraphe 2, du règlement (CE) nº 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données[1] (ci-après le «règlement»). La notification concerne le suivi et l'analyse quantitative des données à caractère personnel des personnes ayant tenu des propos sur la BCE sur les réseaux sociaux. Ces tâches sont effectuées par la division «Relations avec les médias» de la direction générale Communication (DG/C-RMG) de la BCE.

S'agissant d'un nouveau traitement, le délai de deux mois au terme duquel le CEPD doit rendre un avis s'applique par conséquent[2].

2. Faits

La BCE envisage de faire appel à un prestataire externe qui sera chargé de fournir des services de veille sur les réseaux sociaux. La BCE prévoit l'acquisition d'un outil/d'une plate-forme standard de veille sur les réseaux sociaux qui permettra à l'équipe de veille médiatique (MMT), qui fait partie de la DG/C, d'assurer une surveillance et un suivi des commentaires publiés sur des sujets relatifs à la BCE sur différents réseaux sociaux (au moins Twitter, Facebook, Instagram, YouTube, LinkedIn, Google+, Flickr) et d'autres sources en ligne, dont les forums, les blogs et les sites d'actualités en ligne, qui sont gratuits. La BCE entend faire appel à un prestataire situé dans l'Espace économique européen. Si cela devait toutefois s'avérer impossible, tout sera mis en œuvre pour s'assurer que le prestataire offre des garanties suffisantes qu'il se conformera au cadre législatif en matière de protection des données applicable à la BCE. Dans ce cas, la BCE communiquera au CEPD les éléments de preuve nécessaires fournis par le prestataire.

Finalité

Le traitement a pour finalité:

- de comprendre comment la BCE est débattue sur les réseaux sociaux; et
- de surveiller la manière dont la communication de la BCE et sa réputation sont perçues sur les réseaux sociaux afin de garantir une communication plus efficace avec les citoyens.

À cette fin, la BCE souhaite collecter des informations sur les propos qui sont tenus à son égard ou sur des sujets la concernant, sur le ton employé et sur la mesure dans laquelle ces informations sont diffusées.

[1] JO L 8 du 12.1.2001, p. 1.

[2] Le 12 décembre 2017, le CEPD a adressé de nouvelles questions à la BCE. Cette dernière a apporté quelques éclaircissements le 20 décembre 2017, avant d'organiser le 12 janvier 2018 une téléconférence pour fournir de plus amples informations. Le 5 mars 2018, le projet d'avis a été transmis à la BCE pour lui permettre de formuler ses observations. La BCE a rendu réponse le 20 mars 2018.

Personnes concernées
Tous les internautes dont les messages, etc. sont analysés à l'aide de l'outil de veille sur les réseaux sociaux: initiateurs de messages/tweets, influenceurs[3], journalistes, universitaires, banquiers et politiciens.

Base juridique
Le descriptif des tâches de la DG/C[4] de la BCE prévoit en particulier que la division «Relations avec les médias» «*réalise un suivi quotidien des questions de communication soulevées dans les médias et procède à une analyse régulière des lacunes et des défis en matière de communication dans le paysage médiatique mondial*».

En outre, la notification indique que les données collectées et traitées sont mises à la disposition du public à partir des messages postés par les personnes qui ont accepté les conditions générales des plates-formes de réseaux sociaux mentionnées ci-dessus. La notification renvoie au consentement implicite des personnes concernées au titre de l'article 5, point d), du règlement.

Procédure et données traitées
La plate-forme de veille sur les réseaux sociaux sera disponible en permanence (24 heures sur 24, sept jours sur sept et 365 jours par an) pour au moins 50 utilisateurs de la BCE, qui pourront effectuer un nombre illimité de requêtes de recherche. Les résultats des requêtes de recherche feront apparaître les messages postés sur les réseaux sociaux au cours des 30 derniers jours au minimum et la plate-forme offrira diverses fonctionnalités d'analyse des catégories suivantes de données agrégées:

- le volume de couverture, de portée et de popularité;
- le sentiment (négatif/positif);
- les mots et les sujets les plus fréquents;
- l'activité (nombre de «j'aime», de favoris, de commentaires, de partages des utilisateurs sur un sujet particulier);
- les caractéristiques démographiques des auteurs de messages (langue maternelle, pays d'origine et genre),
- les données et l'heure des messages postés pour voir l'évolution au fil du temps.

En outre, les tweets ou les messages de certains influenceurs pourraient être repris dans une analyse.

Les spécialistes en communication de la DG/C analyseront les informations susmentionnées et établiront des rapports.

Destinataires
Le personnel de la DG/C selon le principe du besoin d'en connaître, les membres du directoire de la BCE, les cadres supérieurs de la BCE et le secrétaire général des services de la BCE.

[3] Institutions ou personnes, fortes d'une pertinence, d'une portée et d'une résonance (multiplicateurs), qui écrivent sur la BCE.
[4] Le descriptif des tâches est une décision formelle du directoire (il a été adopté par le secrétaire général des services de la BCE, sur la base d'une délégation accordée par le directoire).

Droit à l'information
D'après la notification, la BCE fournira des informations sur son site internet comme suit: *«La BCE surveille l'activité liée aux sujets couvrant ses tâches sur les réseaux sociaux et à l'utilisation de ses propres réseaux sociaux. Les données à caractère personnel des utilisateurs des réseaux sociaux pourraient être collectées si les utilisateurs font des commentaires sur des sujets relatifs à la BCE ou utilisent les propres réseaux sociaux de la BCE.»*

Droits d'accès et de rectification
La notification indique que, conformément à l'article 20, paragraphe 2, du règlement, aucune procédure spécifique n'est prévue, étant donné que le traitement est réalisé à seule fin d'établir des statistiques.

Politique de conservation
Les données à caractère personnel, qui sont analysées, ne seront pas conservées. Seuls les rapports contenant des données agrégées et des commentaires personnels seront conservés pour une durée indéterminée.

Mesures de sécurité
[...]

3. Aspects juridiques

3.1. Contrôle préalable

Le traitement en question des données à caractère personnel est effectué par une institution de l'Union européenne, la BCE. En outre, le traitement est à la fois automatisé (recherches effectuées à l'aide d'un outil numérique) et manuel – qui fait partie ou est destiné à faire partie d'un fichier (analyse et utilisation des résultats sous la forme de rapports). Par conséquent, le règlement est applicable.

Le suivi et l'analyse porteront sur les catégories de données agrégées susmentionnées. Nombre des influenceurs qui écrivent sur la BCE sont des personnes publiques (journalistes, professeurs, banquiers, etc.). Il peut toutefois y avoir quelques exceptions, les tweets ou les messages de personnes non publiques pouvant être repris dans les rapports. Ces personnes peuvent être indirectement identifiables à partir de leurs commentaires, de leurs appréciations ou de leur langue maternelle. Il s'ensuit que toutes les informations suivies et analysées par la BCE sont des données à caractère personnel se rapportant à des personnes physiques (publiques ou non) au sens de l'article 2, point a), du règlement.

Le traitement porte sur différentes sources de données à caractère personnel provenant d'utilisateurs des réseaux sociaux, qui sont extraites de différentes plates-formes de réseaux sociaux. Le traitement a pour finalité de surveiller les propos et les réactions de différents utilisateurs des réseaux sociaux à l'égard de la BCE. Par conséquent, le traitement en question met en relation différentes sources de données provenant de différentes plates-formes de réseaux sociaux et est susceptible de présenter des risques au regard des droits et libertés des utilisateurs concernés au sens de l'article 27, paragraphe 2, point c), du règlement. Le

traitement est soumis à un contrôle préalable du CEPD, car il relève de la catégorie des traitements à risque[5].

3.2 Licéité

La licéité d'un traitement doit être justifiée sur la base de l'une des cinq conditions légales prévues à l'article 5 du règlement.

Comme souligné à juste titre dans la notification, le traitement en question est considéré comme licite au sens de l'article 5, point a), du règlement.

L'article 5, point a), du règlement requiert le respect de deux conditions: le traitement doit être basé sur les traités ou sur un acte législatif de l'Union européenne et il doit être nécessaire à l'exécution d'une mission de la BCE effectuée dans l'intérêt public sur la base des traités. Le CEPD estime que la mission de la DG/C de la BCE consistant à effectuer un suivi quotidien des questions de communication soulevées dans les médias, comme le prévoit le descriptif des tâches de la BCE, peut justifier le traitement tant que des garanties suffisantes et spécifiques sont prévues conformément au règlement (voir le point ci-dessous sur la qualité des données et les autres recommandations).

La notification indique que le traitement peut également être fondé sur le consentement implicite des personnes concernées au titre de l'article 5, point d), du règlement.

Le «consentement implicite» n'est pas valable en vertu du règlement. L'article 5, point d), du règlement exige expressément que les personnes concernées donnent «indubitablement» leur consentement avant que leurs données à caractère personnel ne soient traitées. Cela signifie que le consentement des personnes concernées doit être une manifestation libre, spécifique et informée par laquelle elles acceptent que leurs données à caractère personnel soient collectées au cours de toutes les différentes étapes du traitement[6]. L'accès aux services de réseaux sociaux est souvent accordé sous réserve d'accepter que le fournisseur de ces services et ses affiliés puissent traiter de diverses façons les données à caractère personnel. Cela ne signifie pas que les utilisateurs consentent à ce que d'autres responsables du traitement, tels que la BCE, traitent leurs données à caractère personnel.

Les utilisateurs sont souvent dans l'impossibilité d'utiliser les services de réseaux sociaux s'ils ne consentent pas à l'utilisation et/ou au transfert de leurs données par le fournisseur des services à d'autres fins (publicité comportementale ou revente à des tiers, par exemple). Cela signifie que leur libre consentement est discutable. Indépendamment de la question de savoir si le consentement des utilisateurs au traitement de leurs données par le fournisseur de services de réseaux sociaux est valable, il semble qu'un tel consentement ne saurait couvrir le traitement par la BCE.

---

5 L'article 27, paragraphe 2, du règlement dresse une liste des traitements susceptibles de présenter des risques au regard des droits et libertés des personnes concernées du fait de leur nature, de leur portée ou de leurs finalités, y compris, au point c), les traitements permettant des interconnexions non prévues en vertu de la législation nationale ou de l'Union européenne entre des données traitées pour des finalités différentes.

6 Conformément à l'article 2, point h), du règlement, on entend par «consentement de la personne concernée» «*toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement*».

Recommandation:
la BCE devrait supprimer les références à l'article 5, point d), du règlement et au «consentement implicite». Le traitement en question ne peut se fonder que sur l'article 5, point a), du règlement, tant que la BCE offre des garanties suffisantes (voir ci-dessous).

3.3 Qualité des données

Le CEPD rappelle que la BCE est tenue de respecter le principe de la qualité des données prévu à l'article 4, paragraphe 1, point c), du règlement qui dispose que «*les données à caractère personnel doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement*».

La BCE devrait veiller, dans les termes du contrat (voir point 3.4), à ce que le prestataire externe applique rigoureusement les principes de nécessité et de proportionnalité lorsqu'il collecte différentes catégories de données des utilisateurs. Le prestataire externe devrait limiter la collecte des données à caractère personnel sur les différentes plates-formes de réseaux sociaux à celles qui sont directement pertinentes et nécessaires au regard de la finalité du traitement (principe de minimisation des données). Le prestataire externe devrait utiliser les moyens les moins invasifs et appliquer les méthodes de protection de la vie privée les plus strictes afin d'atténuer le risque d'atteinte à la vie privée des utilisateurs. Concrètement, le prestataire externe devrait éviter, par exemple, de collecter des messages et des tweets clairement identifiables de personnes non publiques susceptibles, comme il a été souligné ci-dessus, de dévoiler directement ou indirectement leur identité.

Recommandation:
la BCE devrait veiller à ce que le prestataire externe ne collecte que les données nécessaires et proportionnées à la finalité du traitement, à savoir la veille sur les réseaux sociaux, sans risquer de porter atteinte à la vie privée des utilisateurs non publics au sens de l'article 4, paragraphe 1, point c), du règlement.

3.4 Responsable du traitement et sous-traitant

La BCE conclura un contrat avec un prestataire externe qui sera chargé d'effectuer une veille sur les réseaux sociaux pour le compte de sa DG/C.

Conformément à l'article 23 du règlement, le prestataire externe agira pour le compte de la BCE. Par conséquent, il doit être considéré comme le sous-traitant, tandis que la BCE est le responsable du traitement. Cela signifie que la BCE est l'institution de l'Union européenne chargée de déterminer les finalités et les moyens du traitement [article 2, point d), du règlement] et que le prestataire externe ne doit effectuer le traitement que sur instruction de la BCE [article 23, paragraphe 2, point a)].

En particulier, la BCE, en tant que responsable du traitement (article 4, paragraphe 2, du règlement), devrait énoncer dans le contrat les conditions suivantes:

i. le prestataire externe ne doit traiter les données à caractère personnel que sur instruction documentée de la BCE;

ii. la BCE doit indiquer clairement l'objet et la durée du traitement;

iii. la BCE doit préciser la nature et la finalité du traitement;

iv. la BCE doit mentionner le type de données à caractère personnel et les catégories de personnes concernées;

v. le prestataire externe ne doit traiter les données qu'au regard de la finalité pour laquelle elles sont collectées et ne pas traiter les données à d'autres fins incompatibles (transfert de données à d'autres entreprises à des fins commerciales, par exemple);

vi. le prestataire externe ne doit pas être autorisé à transférer des informations traitées ou à externaliser un service à un sous-traitant ou à un prestataire de services tiers, sauf si la BCE l'y autorise;

vii. le prestataire externe doit être en mesure de garantir les droits d'accès et de rectification des personnes concernées en adoptant des mécanismes appropriés leur permettant d'exercer leurs droits (voir point 3.5 pour plus de précisions);

viii. le prestataire externe doit appliquer le délai de conservation des données demandé par la BCE (voir point 3.6);

ix. le prestataire externe ne peut engager un sous-traitant qu'après autorisation écrite de la BCE et tout sous-traitant doit être soumis aux mêmes obligations de protection des données que le prestataire externe;

x. le prestataire externe doit veiller à ce que les personnes autorisées à traiter des données à caractère personnel soient soumises à des obligations de confidentialité;

xi. le prestataire externe doit aider la BCE à démontrer qu'elle respecte le règlement applicable sur la protection des données et à respecter ses obligations de notification en cas de violation de données.

En ce qui concerne les obligations du prestataire externe en matière de confidentialité, de protection des données et de mesures de sécurité prévues à l'article 23, paragraphe 2, point b), du règlement, la BCE doit veiller à ce que des dispositions spécifiques soient ajoutées au contrat concernant ces obligations. En ce qui concerne les obligations en matière de confidentialité et de sécurité, compte tenu du fait que le prestataire externe sera établi dans l'un des États membres, il devrait en principe être soumis aux articles 28 et 32 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE[7].

Le CEPD attire l'attention de la BCE sur les changements à venir[8] énoncés à l'article 29 de la proposition de nouveau règlement sur la protection des données pour les institutions et organes

[7] http://eur-lex.europa.eu/legal-content/FR/TXT/ELI/?eliuri=eli:reg:2016:679:oj

[8] Voir également la lettre du CEPD adressée à toutes les institutions de l'Union européenne le 12 octobre 2017 (dossier 2016-1153 du CEPD) les informant des changements relatifs aux sous-traitants. Il convient de noter que, bien que les législateurs n'aient pas encore conclu les négociations sur la proposition de règlement pour les institutions de l'Union européenne, le texte de l'article 29 est stable et le CEPD a déjà invité dans cette lettre les institutions et organes de l'Union européenne à commencer à se préparer aux changements prévus.

de l'Union européenne[9]. En particulier, le CEPD recommande vivement que toute demande d'offre ou procédure de passation de marché soit déjà conforme au cadre juridique révisé. Il en va de même pour les conditions du contrat. Il est également dans l'intérêt tant du responsable du traitement que du sous-traitant d'énoncer clairement leurs obligations respectives dans le contrat régissant le traitement.

En outre, si le contrat est attribué à une entité située dans un pays non membre de l'Union européenne/de l'Espace économique européen[10] sans qu'aucune décision constatant le caractère adéquat du niveau de protection soit prise, il convient de garantir un niveau de protection des données équivalent aux garanties prévues par le règlement actuel ou le nouveau règlement applicable aux institutions et organes de l'Union européenne. Pour atténuer les risques potentiels, le CEPD recommande que la BCE examine les mesures organisationnelles, techniques et informatiques du prestataire ou des sous-traitants afin de procéder à une évaluation approfondie des risques en matière de sécurité.

Recommandation:
la BCE devrait veiller à ce que toutes les conditions susmentionnées soient énoncées dans le contrat conclu avec le prestataire externe conformément à l'article 23 du règlement.

3.5 Droits d'accès et de rectification

Conformément à l'article 4, paragraphe 1, point d), du règlement, la BCE doit veiller à ce que les données des internautes soient exactes et mises à jour. Elle doit donc prendre toutes les mesures raisonnables pour que les données inexactes ou incomplètes, au regard de la finalité du traitement, soient effacées ou rectifiées. Cela signifie qu'il incombe à la BCE de veiller à ce que les internautes soient en mesure d'exercer leurs droits d'accès (article 13 du règlement) et de rectification (article 14 du règlement).

La notification indique que, conformément à l'article 20, paragraphe 2, du règlement, aucune procédure spécifique n'est prévue, étant donné que le traitement est réalisé à seule fin d'établir des statistiques.

Le CEPD souligne que le traitement comprend deux phases: la première concerne l'analyse initiale des informations collectées par le prestataire externe aux fins d'établir des statistiques et la seconde concerne l'établissement de rapports par la BCE à partir de ces statistiques susceptibles de contenir des commentaires identifiables.

Première phase du traitement
Conformément à l'article 20, paragraphe 2, du règlement, lorsque les données sont traitées exclusivement aux fins de la **recherche statistique**, les droits d'accès et de rectification ne s'appliquent pas, sous réserve i) qu'il n'existe manifestement **aucun risque d'atteinte à la vie privée des personnes concernées** et ii) que le responsable du traitement offre **des garanties**

[9] Proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) nº 45/2001 et la décision nº 1247/2002/CE, COM(2017) 8 final.
[10] Il en va de même pour les entités possédant des succursales/bureaux dans un pays non membre de l'Union et ayant accès aux données collectées ou pour le prestataire qui sous-traiterait à une entité située en dehors de l'Union européenne.

juridiques appropriées, qui excluent notamment que les données puissent être utilisées aux fins de mesures ou de décisions se rapportant à des personnes déterminées.

Le prestataire externe traitera les données, pour le compte de la BCE, à des fins purement statistiques. Étant donné que le prestataire externe extraira des données agrégées et que la BCE établira des rapports sur la base de cette extraction, il ne semble pas y avoir de risque d'atteinte à la vie privée des internautes, tant qu'aucun commentaire identifiable ne figure dans les rapports.

Quant à la question de savoir si le responsable du traitement (BCE) offrira des garanties juridiques appropriées, la BCE devrait veiller à ce que les données ne soient traitées qu'à des fins statistiques et qu'elles ne soient pas utilisées pour prendre des décisions individuelles sur les internautes. La BCE devrait veiller à ce que le prestataire externe prenne les mesures de sécurité appropriées (voir point 3.8 relatif à la sécurité).

Par conséquent, les articles 13 et 14 ne s'appliquent pas au cours de la première phase du traitement, sous réserve que la BCE veille à ce que le prestataire externe adopte des garanties juridiques appropriées, comme le prévoit l'article 20, paragraphe 2, du règlement.

Seconde phase du traitement

Si une personne concernée identifie un de ses commentaires/messages/tweets dans le rapport et souhaite exercer ses droits d'accès et de rectification, les articles 13 et 14 du règlement s'appliquent au cours de cette phase particulière du traitement. Par conséquent, la BCE devrait prendre toutes les mesures raisonnables pour garantir ces droits et veiller à ce que les données à caractère personnel des utilisateurs soient exactes et mises à jour.

Recommandation:

la BCE devrait veiller à ce que:

i) lors de la première phase du traitement (compilation d'informations à des fins statistiques par le prestataire externe), les internautes puissent exercer leurs droits d'accès et de rectification en contactant directement le prestataire externe; et

ii) lors de la seconde phase du traitement (établissement de rapports susceptibles de contenir des commentaires identifiables), les internautes puissent exercer leurs droits d'accès et de rectification en contactant directement la BCE.

3.6 Conservation des données

L'article 4, paragraphe 1, point e), du règlement dispose, à titre de principe général, que les données à caractère personnel ne doivent pas être conservées sous une forme permettant l'identification des personnes concernées pendant une durée excédant celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement.

La notification indique que les données à caractère personnel, qui sont analysées, ne seront pas conservées. Seuls les rapports contenant des données agrégées et des commentaires personnels le seront.

Il n'existe aucune information sur le délai de conservation des données à caractère personnel stockées par le prestataire externe ou des rapports conservés par la BCE (dans la mesure où ils contiennent des données à caractère personnel). Conformément à l'article 4, paragraphe 1,

point c), du règlement, la BCE est tenue de fixer dans le contrat conclu avec le prestataire externe un délai de conservation maximal pour les données traitées, qui soit nécessaire au regard de la finalité pour laquelle ces données ont été collectées ou traitées ultérieurement (voir point 3.3 ci-dessus). En outre, conformément à l'article 4, paragraphe 1, point e), du règlement, la BCE doit procéder à une appréciation du délai pendant lequel il est nécessaire de conserver les rapports à des fins statistiques, actuelles et futures, et établir un délai de conservation maximal.

Recommandation:
la BCE devrait fixer un délai de conservation maximal pour i) les données traitées par le prestataire externe et ii) les rapports (dans la mesure où ils contiennent des données à caractère personnel).

3.7 Information des internautes

Les articles 11 et 12 du règlement portent sur les informations à fournir aux personnes concernées afin de garantir un traitement loyal et transparent de leurs données à caractère personnel. Dans le cas présent, les données à caractère personnel ne sont pas collectées directement auprès des internautes, mais sur différentes plates-formes de réseaux sociaux. Par conséquent, l'article 12 du règlement s'applique.

La BCE a indiqué dans la notification qu'elle fournira des informations sur son site internet. Avant toute chose, le CEPD tient à préciser que la simple publication d'une déclaration de confidentialité ne suffit pas à se conformer aux obligations d'information prévues à l'article 12, paragraphe 1, du règlement. L'article 12, paragraphe 2, du règlement prévoit toutefois une exception en vertu de laquelle ces obligations ne s'appliquent pas lorsque, en particulier pour un traitement à finalité statistique, l'information des internautes se révèle impossible ou implique des efforts disproportionnés. Dans ce cas, le responsable du traitement doit prévoir des garanties appropriées après avoir consulté le CEPD.

En principe, la BCE ne disposera pas des coordonnées des utilisateurs dont les messages seront analysés par le prestataire externe et n'en aura pas besoin au regard des finalités du traitement. La collecte et le traitement de nouvelles données à caractère personnel dans le seul but d'informer les personnes concernées iraient à l'encontre du principe de minimisation des données. En ce sens, il serait disproportionné de collecter les coordonnées dans le seul but d'informer directement les personnes concernées. Par conséquent, la BCE peut se prévaloir dans le présent cas de l'exemption prévue à l'article 12, paragraphe 2, du règlement.

Lorsque les responsables du traitement se fondent sur l'article 12, paragraphe 2, du règlement pour ne pas informer directement les personnes concernées, ils doivent prévoir des garanties appropriées. Une garantie appropriée serait que la BCE rédige une déclaration de confidentialité et la publie sur son site internet.

En ce qui concerne le contenu de la déclaration de confidentialité, la BCE devrait fournir des informations claires et complètes sur tous les éléments énumérés à l'article 12 du règlement. Elle devrait également:

i) préciser son rôle et celui du prestataire externe;

ii) mentionner la possibilité pour les internautes d'exercer leurs droits d'accès et de rectification de leurs données en contactant directement le prestataire externe, comme expliqué au point 3.5; et

iii) indiquer le délai de conservation des données conservées par la BCE et par le prestataire externe, comme expliqué au point 3.6.

En vue de l'application de l'article 12, paragraphe 2, du règlement et afin de garantir un traitement loyal et transparent, le CEPD recommande que la BCE indique dans la déclaration de confidentialité qu'il lui est impossible d'informer directement les internautes ou que cela implique des efforts disproportionnés, étant donné qu'elle ne dispose pas, en principe, de leurs coordonnées.

Recommandation:
la BCE devrait inclure toutes les recommandations susmentionnées dans la déclaration de confidentialité et la publier de manière bien visible sur son site internet avant le lancement du traitement.

3.8 Sécurité

L'article 22 du règlement oblige le responsable du traitement à mettre en œuvre les mesures techniques et organisationnelles appropriées pour assurer un niveau de sécurité approprié au regard des risques présentés par le traitement.

Même si la BCE ne traite directement aucune donnée à caractère personnel, elle est tenue de respecter l'article 23 du règlement: «[l]*orsque le traitement est effectué pour son compte, le responsable du traitement choisit un sous-traitant qui apporte des garanties suffisantes au regard des mesures de sécurité technique et d'organisation prévues par l'article 22 et veille au respect de ces mesures*». Par conséquent, le prestataire externe devrait rendre compte à la BCE de l'analyse des risques en matière de sécurité des informations effectuée et des mesures de sécurité retenues pour gérer les risques recensés pour la plate-forme de veille sur les réseaux sociaux. À cette fin, la BCE devrait obtenir une garantie formelle (attestation de sécurité, par exemple) que le prestataire externe respecte effectivement les obligations qui lui incombent en matière de confidentialité et de sécurité des données à caractère personnel qui lui sont confiées.

Recommandation:
la BCE devrait veiller à ce que le prestataire externe mette en œuvre les mesures techniques et organisationnelles appropriées pour assurer un niveau de sécurité approprié au regard des risques présentés par le traitement en question.

4. Conclusion

Rien ne porte à croire que les dispositions du règlement sont violées, pour autant que les recommandations ci-après soient pleinement prises en considération. La BCE devrait notamment:

- supprimer de la notification l'article 5, point d), du règlement et toute référence au consentement implicite. Le traitement en question ne peut se fonder que sur l'article 5, point a), du règlement, tant que la BCE offre des garanties suffisantes (point 3.3);

- énoncer toutes les conditions indiquées au point 3.4 dans le contrat conclu avec le prestataire externe, conformément à l'article 23 du règlement;

- veiller à ce que les internautes puissent exercer leurs droits d'accès et de rectification en contactant directement le prestataire externe et la BCE (point 3.5);

- fixer un délai de conservation maximal pour i) les données traitées par le prestataire externe et ii) les rapports (point 3.6);

- inclure de manière claire et exhaustive toutes les recommandations formulées au point 3.7 dans la déclaration de confidentialité et publier celle-ci de manière bien visible sur son site internet avant le lancement du traitement; et

- veiller à ce que le prestataire externe mette en œuvre les mesures techniques et organisationnelles appropriées pour assurer un niveau de sécurité approprié au regard des risques présentés par le traitement en question (point 3.8).

Dans le cadre de la procédure de suivi, veuillez envoyer au CEPD une copie de la déclaration de confidentialité et des documents relatifs à la sécurité pour le traitement en question, dans un délai de trois mois, pour démontrer que les recommandations du CEPD qui précèdent ont été mises en œuvre.

Fait à Bruxelles, le 21 mars 2018

(signé)

Wojciech Rafał WIEWIÓROWSKI