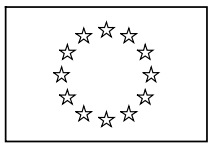

COMMISSION DES COMMUNAUTÉS EUROPÉENNES

Bruxelles, le 22.01.2004
COM(2004) 28 final

COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPEEN, AU CONSEIL, AU COMITE ECONOMIQUE ET SOCIAL EUROPEEN ET AU COMITE DES REGIONS

sur les communications commerciales non sollicitées ou «spam»

TABLE DES MATIÈRES

COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPEEN,AU CONSEIL, AU COMITE ECONOMIQUE ET SOCIAL EUROPEEN ET AU COMITE DES REGIONS

sur les communications commerciales non sollicitées ou «spam»

(Texte présentant de l'intérêt pour l'EEE)

RESUME

Les communications commerciales non sollicitées par courrier électronique, également connues sous le nom de «spam», ont atteint des proportions inquiétantes. On estime désormais que plus de 50 % du courrier électronique échangé au niveau mondial est constitué de «spam». Le taux de croissance de ce phénomène est encore plus inquiétant puisqu'en 2001, la proportion de «spam» n'était «que» de 7 %.

Le «spam» est un problème pour de nombreuses raisons: atteinte à la vie privée, tromperie des consommateurs, protection des mineurs et de la dignité humaine, surcoûts pour les entreprises, perte de productivité. Plus généralement, ce phénomène mine la confiance des consommateurs, qui est une condition préalable au succès du commerce électronique, des services en ligne et même, de la société de l'information.

En prévision de ce danger, l'UE a adopté, en juillet 2002, la directive 2002/58/CE (directive «vie privée et communications électroniques») qui a introduit dans l'ensemble de l'UE le principe dit «opt-in», c'est-à-dire le consentement préalable obligatoire de l'abonné pour l'envoi de courrier électronique à des fins commerciales (y compris messages SMS ou MMS), ainsi que des garanties complémentaires pour les consommateurs. L'échéance pour la mise en œuvre de la directive «vie privée et communications électroniques» était fixée au 31 octobre 2003. Des procédures d'infraction ont été ouvertes à l'encontre de plusieurs États membres qui n'ont pas notifié de mesures de transposition à la Commission.

L'adoption de la législation est certes un premier pas nécessaire, mais elle ne constitue qu'une partie de la réponse. La présente communication répertorie une série d'actions nécessaires pour compléter la réglementation de l'UE et faire de « l'interdiction du spam» une réalité.

Il n'y a malheureusement pas de remède miracle contre le spam. Les actions énumérées dans la présente communication sont axées notamment sur l'application effective de la législation par les États membres et les pouvoirs publics, sur des solutions techniques et l'autorégulation de la part de l'industrie, et sur la sensibilisation des consommateurs. La dimension internationale est également mise en évidence, étant donné qu'une grande quantité de «spam» provient de l'extérieur de l'Union européenne.

Bien que ces actions reflètent largement le consensus qui s'est dégagé au cours de 2003, comme cela a été confirmé lors d'un atelier public qui a eu lieu en octobre 2003, un consensus sur leur mise en œuvre sera également essentiel. La prolifération du spam ne sera enrayée que si tous les acteurs concernés jouent leur rôle, depuis les États membres et les pouvoirs publics jusqu'aux consommateurs et aux utilisateurs de l'internet et des communications électroniques, en passant par les entreprises.

Certaines des actions envisagées ont un coût certain, mais c'est le prix à payer si l'on veut que le courrier électronique et les services électroniques restent un outil de communication efficace. La mise en œuvre des actions répertoriées dans la présente communication contribuera dans une large mesure à réduire le volume de «spam», dans l'intérêt de la société de l'information, de nos citoyens et de nos économies.

CONTEXTE ET OBJECTIF

L'envoi par courrier électronique de communications commerciales non sollicitées[1], également désigné par le terme «spam», est reconnu comme l'un des plus graves problèmes que connaît l'internet actuellement. Ce phénomène a atteint des proportions inquiétantes. Le risque existe que des utilisateurs courrier électronique ou de SMS arrêtent d'utiliser la messagerie électronique – qui est l'une des applications les plus populaires de l'internet – ou les services mobiles, ou les utilisent d'une manière plus limitée. D'une manière plus générale, étant donné que l'internet et d'autres moyens de communications électroniques (par ex. l'accès à large bande, l'accès sans fil, les communications mobiles) devraient constituer un élément essentiel de la croissance de la productivité dans une économie moderne, le «spam» exige encore plus d'attention.

Bien qu'il existe un consensus sur le fait qu'il est nécessaire d'agir avant que la prolifération du spam n'annule les avantages qu'apportent la messagerie électronique et les autres services en ligne aux entreprises et aux individus, la détermination des meilleurs moyens de lutte n'est pas une évidence. Plus important encore, il n'existe aucun remède miracle. La prolifération du spam n'aura de chance d'être enrayée efficacement que si tous les acteurs concernés jouent leur rôle, depuis les États membres et les autorités compétentes jusqu'aux consommateurs et aux utilisateurs de l'internet et des communications électroniques, en passant par les entreprises.

La présente communication recense des actions à mener sur différents fronts (juridique, technique et sensibilisation), en se fondant sur la directive 2002/58/CE, laquelle établit un régime de consentement préalable («opt-in») que les États membres devaient mettre en œuvre pour les communications commerciales pour le 31 octobre 2003[2].

Cette série d'actions est notamment axée sur la mise en œuvre et le contrôle d'application effectifs de la directive par les États membres, sur les mesures techniques, sur l'autorégulation du secteur d'activité, sur la sensibilisation des consommateurs et sur la coopération internationale. La dimension internationale est en effet cruciale, étant donné qu'un volume considérable de spam semble provenir de l'extérieur de l'Union européenne, et notamment d'Amérique du Nord[3].

---

1 La présente communication ne couvre pas les communications non sollicitées hors ligne, telles que le courrier (postal) non sollicité.

2 Voir notamment l'article 13 de la directive 2002/58/CE (directive «vie privée et communications électroniques» (cf. le chapitre 2 ci-dessous).

3 Par exemple, les initiatives «boîte à spam» organisées en 2002 respectivement par la Commission nationale de l'informatique et des libertés (CNIL) en France et par la Commission de la protection de la vie privée (CPVP) en Belgique semblent confirmer que les États-Unis et, dans une moindre mesure, le Canada, sont la principale source de «spam». Les conclusions de la CPVP sont disponibles à l'adresse http://www.privacy.fgov.be/publications/spam_4-7-03_fr.pdf; le rapport de la CNIL est disponible à l'adresse http://www.cnil.fr/thematic/docs/internet/boite_a_spam.pdf. Voir également: CNUCED, Rapport sur le commerce électronique et le développement 2003, New York et Genève, 2003, p. 27.

Ces actions reflètent largement le consensus qui s'est dégagé au cours de l'année 2003, comme cela a été confirmé lors d'un atelier public organisé en octobre 2003[4]. Un consensus dans ce domaine est d'autant plus important qu'il appartient essentiellement aux parties concernées, avec l'appui de la Commission dans la mesure du possible, de mettre en œuvre les actions répertoriées, dans l'intérêt de la société de l'information, de son industrie et de ses utilisateurs.

Structure du document

Le document répertorie différents aspects du problème que constitue le spam et propose des mesures spécifiques à prendre vis-à-vis de chacun de ces aspects. Des meilleures pratiques ont également été mises en évidence chaque fois que l'utilité s'en faisait sentir.

Les actions proposées sont présentées selon la structure suivante:

- **Actions de mise en œuvre et de contrôle d'application :** elles s'adressent principalement aux gouvernements et aux pouvoirs publics, dans des domaines comme les recours et sanctions, les mécanismes de dépôt de plainte, les plaintes transfrontalières, la coopération avec les pays tiers, la surveillance (chapitre 3).

- **Actions d'autorégulation et actions techniques :** elles concernent surtout les acteurs du marché, dans des domaines comme les dispositions contractuelles, les codes de conduite, les pratiques de marketing acceptables, les labels, les systèmes alternatifs de règlement des conflits, les solutions techniques telles que le filtrage, la sécurité (chapitre 4).

- **Actions de sensibilisation :** elles englobent la prévention, l'éducation des consommateurs, les mécanismes de plainte, à adopter par les gouvernements et les pouvoirs publics, les acteurs du marché, les associations de consommateurs et assimilés (chapitre 5).

Toutes ces actions sont résumées dans un tableau qui figure à la fin de la présente communication. Elles sont liées les unes aux autres de plusieurs manières. Il faudrait dans la mesure du possible les mettre en œuvre en parallèle et de manière intégrée.

Avant de passer à la présentation de ces actions, les chapitres suivants analysent brièvement le phénomène du spam en tant que tel (chapitre 1) et rappelent les nouvelles règles applicables depuis le 31 octobre 2003 (chapitre 2).

---

[4] Un document de réflexion sur les communications commerciales non sollicitées ou «spam» a été distribué avant l'atelier. Ce document de réflexion était lui-même fondé sur des débats antérieurs dans le cadre du Comité des communications (COCOM) et avec le groupe de travail «article 29» sur la protection des données. Les membres du COCOM et du groupe de travail «article 29» sur la protection des données ont fourni des informations en réponse à un questionnaire. Plusieurs associations sectorielles ou entreprises ont également réagi, qu'il s'agisse de fournisseurs de services internet et d'opérateurs de communications (mobiles et fixes), de sociétés de prospection directe ou de publicitaires, ou encore de fabricants de matériel informatique et de logiciels.

1. LE PROBLEME DU SPAM

Spam: de quoi s'agit-il?

Le terme spam est plus souvent utilisé qu'il n'est défini. En bref, ce terme est fréquemment utilisé pour désigner l'envoi, souvent massif, de messages électroniques non sollicités. La nouvelle directive ne définit pas le terme spam et ne l'utilise pas. Elle fait appel aux concepts de «communications non sollicitées» transmises par «courrier électronique», «à des fins de prospection directe» qui, considérés ensemble, couvrent de fait la plupart des types de spam. La notion de spam est donc utilisée dans la présente communication comme synonyme de «courrier électronique commercial non sollicité».

Il faut remarquer que la notion de «courrier électronique» elle-même recouvre non seulement les messages électroniques traditionnels utilisant le protocole SMTP (courriel), mais aussi les SMS, les MMS et même toute forme de communication électronique pour laquelle la participation simultanée de l'expéditeur et du destinataire n'est pas requise (voir le chapitre 2 ci-dessous).

1.1. L'ampleur du problème

Le spam a atteint des proportions inquiétantes. Même si les statistiques varient, on estime généralement que plus de la moitié du trafic mondial de courriel est constituée de spam.

Le taux de croissance de ce phénomène est encore plus préoccupant. Selon les estimations, en 2001, le spam ne représentait en effet «que» 7 % du trafic mondial de courrier électronique. Cette estimation est passée à 29 % en 2002, et les projections pour 2003 tablent sur 51 % de spam.

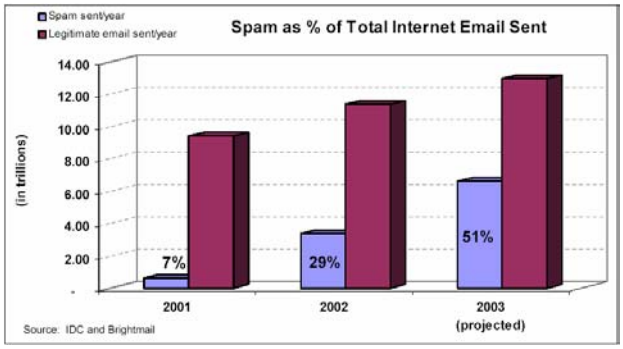

Figure n° 1: proportion de spam par rapport à l'ensemble du courrier électronique envoyé par l'internet

Il peut y avoir des variations considérables entre les catégories d'utilisateurs et entre les régions du monde (à la Commission européenne, par exemple, on estime que 30 % des messages électroniques venant de l'extérieur sont du spam). En général, toutefois, les chiffres récents concernant l'UE ne sont pas moins préoccupants que les chiffres mondiaux[5].

Bien que les communications non sollicitées ou le spam semblent être moins problématiques actuellement sur les réseaux mobiles (par l'intermédiaire du service SMS, par exemple), des évolutions telles que la transmission de courriels aux téléphones mobiles pourraient augmenter le volume de spam. L'expérience des pays qui connaissent un fort taux d'utilisation des services d'internet mobile i-mode (par ex. le Japon) confirme cette menace.

---

[5] En septembre 2003, la proportion de spam dans l'UE était de 49 %, contre 54 % pour le monde entier à la même période (Source: Brightmail, 2003).

1.2. Pourquoi le spam est-il un problème?

Le spam préoccupe-t-il les gens?

Le nombre de plaintes est une indication des préoccupations exprimées par les utilisateurs. En 3 mois, la «boîte à spam» française avait recueilli 325 000 messages. Une expérience analogue en Belgique a permis de recueillir 50 000 plaintes en deux mois et demi. La boîte à spam permanente gérée par la FTC, dénommée UCE Database, recevait 130 000 messages par jour au début de l'année 2003.

Du point de vue individuel, le spam est une intrusion dans la vie privée. Cette préoccupation est au cœur des nouvelles règles sur les communications non sollicitées décrites dans le chapitre suivant. En outre, le spam est souvent mensonger ou trompeur. Une proportion considérable de spam semble répondre à une volonté d'escroquer les consommateurs par des déclarations mensongères ou trompeuses[6]. Malheureusement beaucoup trop de consommateurs répondent à ce spam trompeur ou mensonger[7]. Les messages à caractère pornographique peuvent également être très choquants[8]. Le nettoyage des boîtes aux lettres électroniques prend du temps et accroît le coût pour l'utilisateur s'il est obligé d'acquérir des logiciels de filtrage et autres.

Le développement du spam a atteint un point où il engendre aussi des coûts considérables pour les entreprises. Il s'agit tout d'abord de coûts directs: le personnel est contraint de nettoyer les boîtesaux lettres électroniques, ce qui réduit son efficacité et sa productivité au travail. Les services informatiques consacrent du temps et de l'argent à essayer de résoudre le problème. Les fournisseurs de services internet (ISP) et les fournisseurs de services de courrier électronique (ESP) doivent acquérir plus de largeur de bande et plus de capacités de stockage pour des messages électroniques indésirables. Il existe également un risque que le spam mette en jeu la responsabilité de celui qui le reçoit (par exemple en cas de contenu préjudiciable trouvé sur le PC d'un employé), ou qui le relaie simplement – et

---

6 Selon un rapport récent de la Federal Trade Commission aux États-unis, 22 % des messages de spam analysés contenaient des informations fausses dans le champ «objet» du message; 42 % contenaient, dans le champ «objet», des allégations mensongères selon lesquelles l'expéditeur avait des relations commerciales ou personnelles avec le destinataire; 44 % de ces messages contenaient des informations fausses dans les champs «expéditeur» ou «objet»; plus de la moitié des messages de spam liés à des questions financières contenaient de fausses informations dans les champs «expéditeur» ou «objet»; dans 40% des cas, le corps du message contenait des signes de mensonge; 90% des offres relatives à des investissements et à des occasions commerciales contenaient des affirmations vraisemblablement fausses; 66 % du spam contenait des informations fausses dans le champ «expéditeur», dans le champ «objet» ou dans le corps du message. (False Claims in Spam, A report by the FTC's Division of Marketing Practices, 30 avril 2003, disponible à l'adresse: http://www.ftc.gov/reports/spam/030429spamreport.pdf)

7 D'après Pew Internet, 7 % des utilisateurs du courrier électronique déclarent avoir passé une commande après réception d'un message électronique non sollicité, et 33 % ont cliqué sur un lien inclus dans un message électronique non sollicité pour obtenir plus d'informations. Même si le pourcentage de consommateurs qui se font escroquer reste relativement faible, ce problème a acquis une nouvelle dimension en raison des économies d'échelle phénoménales que peuvent réaliser des opérateurs sans scrupules en recourant à des messages de spam trompeur ou mensonger. Voir: 'Spam – How It Is Hurting Email and Degrading Life on the Internet', octobre 2003, rapport rédigé par Deborah Fallows pour Pew Internet & American Life Project. Ce rapport est disponible à l'adresse URL suivante: http://www.pewinternet.org/reports/pdfs/PIP_Spam_Report.pdf. Un expéditeur de courrier électronique en masse a récemment déclaré, lors du forum sur le spam organisé par la FTC en avril-mai 2003, qu'il pouvait réaliser des bénéfices même si son taux de réponse était inférieur à 0,0001 %. (Remarques de Timothy J. Muris Chairman, Federal Trade Commission, sommet d'Aspen, Cyberspace and the American Dream, The Progress and Freedom Foundation, 19 août 2003, Aspen, Colorado).

8 Il arrive aussi que des messages de spam contiennent des manifestations de violence gratuite ou des incitations à la haine pour des raisons liées à la race, au sexe, à la religion ou à la nationalité.

involontairement (il est possible que cette personne soit mise à tort sur une liste noire ou voie sa réputation ternie). Le spam entraîne aussi des coûts indirects: certains messages électroniques légitimes, à caractère commercial ou professionnel, ne sont pas livrés en raison des techniques de filtrage anti-spam actuelles (entraînant des cas de «faux positifs»), ou ne sont simplement plus lus en raison de leur association au spam. Le spam est de plus en plus utilisé pour diffuser des virus ce qui peut s'avérer très coûteux pour les entreprises.

Mesurer le coût du spam reste un exercice difficile, notamment pour les particuliers, notamment parce qu'il est difficile d'attribuer une valeur monétaire à certains des préjudices subis. Toutefois, les estimations sont généralement inquiétantes. À titre d'exemple, Ferris Research a estimé qu'en 2002, le spam a coûté aux entreprises européennes 2,5 milliards d'euros uniquement en pertes de productivité[9]. Comme indiqué ci-dessus, le volume de spam s'est considérablement accru depuis 2002. Le fournisseur de logiciels MessageLabs Ltd a estimé le coût du spam pour les entreprises britanniques en juin 2003 à quelque 3,2 milliards de livres[10]. Le spam peut aussi avoir différentes implications en fonction des secteurs concernés. Le secteur juridique, par exemple, peut être particulièrement touché par le spam en raison des informations confidentielles et sensibles qu'il traite.

L'une des conséquences les plus inquiétantes du spam est le fait qu'il mine la confiance des utilisateurs, alors que celle-ci est une condition préalable au succès du commerce électronique et de la société de l'information dans son ensemble. Par ailleurs, le fait qu'un canal de vente au détail soit perçu comme étant utilisé par des escrocs peut avoir un effet sérieux sur la réputation des opérateurs légitimes dans le même secteur. Des chiffres récents concernant les États-Unis, dont l'expérience du spam est plus étendue que celle de l'UE, confirment que beaucoup d'utilisateurs font moins confiance au courrier électronique en raison des grandes quantités de spam qu'ils reçoivent[11].

Plus généralement, l'internet et d'autres moyens de communications électroniques – l'accès à large bande, l'accès sans fil – devraient être un élément déterminant de la croissance de la productivité dans les économies modernes. Or, certaines caractéristiques attractives de ces services – le fait d'être en ligne en permanence, l'accès sans fil – risquent précisémentt d'accroître considérablement le volume de spam reçu ou relayé, en l'absence de mesures de sécurité adéquates. Ainsi, d'une manière assez perverse, la croissance de ces services pourrait entraîner une augmentation du spam si des mesures efficaces ne sont pas mises en œuvre rapidement.

2. RESUME DES REGLES RELATIVES AUX COMMUNICATIONS COMMERCIALES NON SOLLICITEES

2.1. Le régime du consentement préalable («opt-in»)

La directive 2002/58/CE sur la vie privée et les communications électroniques (qui devait être transposée pour le 31 octobre 2003) prévoit que les États membres interdisent l'envoi de messages commerciaux non sollicités par courrier électronique ou par un autre système de messagerie électronique tel que le SMS ou le MMS (Multimedia Messaging Service) sauf si

---

9 Source: Ferris Research, 2003.

10 Ce chiffre et d'autres estimations sont mentionnés dans: «Spam; Report of an Inquiry by the All Party Internet Group», Londres, octobre 2003, p. 8; ce rapport peut être consulté via l'adresse URL suivante: http://www.apig.org.uk.

11 Selon l'enquête récente précitée réalisée par Pew Internet, 25 % des personnes interrogées avaient réduit leur utilisation du courrier électronique à cause des quantités de spam qu'elles recevaient.

l'abonné à ces services de communications électroniques a donné son consentement préalable (article 13, paragraphe 1 de la directive)[12]. Il s'agit du système «opt-in», qui n'était jusqu'ici applicable qu'aux télécopieurs et aux automates d'appel[13].

Le nouveau régime comprend trois règles de base:

Règle n° 1: la prospection directe par courrier électronique est subordonnée au consentement préalable des abonnés. Une exception limitée est prévue pour les courriels (ou les SMS) envoyés par une entreprise à des clients existants concernant les services ou produits analogues qu'elle fournit. Ce régime s'applique aux abonnés qui sont des personnes physiques, mais les États membres peuvent choisir de l'étendre aux personnes morales.

Règle n° 2: il est illicite de camoufler ou de dissimuler l'identité de l'émetteur pour le compte duquel la communication est effectuée.

Règle n° 3: tous les courriels doivent mentionner une adresse de réponse valide où l'abonné peut faire opposition à l'envoi de messages ultérieurs.

Tous les messages électroniques non sollicités ne sont cependant pas interdits. En effet, une exception à cette règle est prévue dans les cas où les coordonnées électroniques pour l'envoi de messages électroniques ou de SMS ont été obtenues dans le cadre d'une vente. On parle dans ce cas d'un « soft opt-in ». Dans le cadre d'une telle relation fournisseur-client, l'entreprise qui a obtenu les données d'un client peut les utiliser à des fins de prospection pour des produits ou services analogues à ceux qu'elle a déjà vendus à ce client. Cette exception a été harmonisée au niveau communautaire, et les États membres n'ont d'autre choix que de la mettre en œuvre. Cette exception doit toutefois être rédigée strictement afin de ne pas compromettre le fonctionnement du régime «opt-in». Néanmoins, même dans ce cas, l'entreprise doit indiquer clairement, dès la collecte des données, que celles-ci peuvent être utilisées à des fins de prospection directe (et, le cas échéant, qu'elles peuvent être transmises à des tiers à cette fin) et elle devrait donner au consommateur le droit de s'y opposer, «sans frais et de manière simple». En outre, chaque message de prospection ultérieur devrait offrir au consommateur un moyen simple et gratuit de s'opposer à l'envoi de messages supplémentaires (régime «opt-out»).

Le régime «opt-in» est obligatoire pour tout envoi de courriels ou SMS à une personne physique à des fins de prospection directe. Les États membres peuvent étendre le régime «opt-in» aux communications destinées aux entreprises (personnes morales). Les États membres qui avaient adopté un régime «opt-out» pour la prospection interentreprises, y compris un système de listes d'opposition, peuvent le conserver. L'application d'un régime différencié en fonction de la nature d'un abonné à un service de courrier électronique peut entraîner, pour l'expéditeur de tels messages, des difficultés spécifiques pour distinguer les personnes morales des personnes physiques.

Pour toutes les catégories de destinataires (personnes physiques et morales), la directive interdit l'envoi de messages de prospection directe qui camouflent ou dissimulent l'identité de l'émetteur. Les messages doivent en outre mentionner une adresse valide à laquelle les destinataires peuvent transmettre une demande visant à obtenir que ces communications cessent[14].

---

12 Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), JO L 201 du 31.7.2002.

13 Pour les appels de prospection commerciale par téléphonie vocale (exception faite des automates d'appel), les États membres peuvent choisir entre une approche «opt-in» ou «opt-out».

14 Article 13, paragraphe 4, de la directive 2002/58/CE.

Le groupe de travail «article 29» sur la protection des données, qui a été créé pour conseiller la Commission et réunit les autorités responsables de la protection des données dans l'UE, examine de plus près certains de ces concepts afin de contribuer à une application uniforme des mesures nationales prises en vertu de la directive 2002/58/CE[15]. Un consensus sur ces questions évitera des différences d'interprétation qui nuiraient au fonctionnement du marché intérieur. D'autres aspects des communications non sollicitées ont été traités dans des documents antérieurs du groupe de travail[16].

2.2. Dispositions d'exécution

Les dispositions de la directive «générale» sur la protection des données concernant les recours juridictionnels, la responsabilité et les sanctions sont applicables aux dispositions de la directive «vie privée et communications électroniques», y compris les dispositions sur les communications non sollicitées[17].

En résumé, les États membres doivent veiller à prévoir, en cas d'infraction, des possibilités de recours et des sanctions. Toute violation des droits garantis par le droit interne doit ouvrir un droit individuel à un recours juridictionnel. Bien que ce recours juridictionnel ne préjuge pas d'éventuelles procédures administratives (qui peuvent être antérieures), celles-ci ne font l'objet d'aucune exigence harmonisée. Tout préjudice subi du fait d'un traitement ou d'un acte illégal doit ouvrir un droit individuel à une indemnisation. Des sanctions doivent être prévues en cas d'infraction, afin d'assurer la mise en œuvre intégrale de la directive.

En d'autres termes, alors que la nature même d'une directive donne aux États membres une marge de manœuvre dans le choix des mesures à prendre pour sa mise en œuvre – y compris les recours et les sanctions – ces mesures doivent assurer la pleine application des dispositions relatives aux communications commerciales non sollicitées.

---

15 Conformément à l'article 15, paragraphe 3 de la directive 2002/58/CE, en liaison avec l'article 30 de la directive 95/46/CE.

16 Voir par exemple l'avis 7/2000 sur la proposition de directive du Parlement européen et du Conseil concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications, du 12 juillet 2000; la recommandation 2/2001 sur certaines exigences minimales relatives à la collecte en ligne de données à caractère personnel dans l'Union européenne. La collecte de données a été examinée dans le document de travail du 21 novembre 2000 intitulé «Le respect de la vie privée sur Internet – Une approche européenne intégrée sur la protection des données en ligne». Ces documents peuvent être consultés à l'adresse URL suivante: http://europa.eu.int/comm/internal_market/privacy/workingroup_fr.htm

17 L'article 15 de la directive 2002/58/CE renvoie au chapitre III de la directive 95/46/CE sur les recours juridictionnels, la responsabilité et les sanctions:
Article 22 – Recours
Sans préjudice du recours administratif qui peut être organisé, notamment devant l'autorité de contrôle visée à l'article 28, antérieurement à la saisine de l'autorité judiciaire, les États membres prévoient que toute personne dispose d'un recours juridictionnel en cas de violation des droits qui lui sont garantis par les dispositions nationales applicables au traitement en question.
Article 23 – Responsabilité
1. Les États membres prévoient que toute personne ayant subi un dommage du fait d'un traitement illicite ou de toute action incompatible avec les dispositions nationales prises en application de la présente directive a le droit d'obtenir du responsable du traitement réparation du préjudice subi.
2. Le responsable du traitement peut être exonéré partiellement ou totalement de cette responsabilité s'il prouve que le fait qui a provoqué le dommage ne lui est pas imputable.
Article 24 – Sanctions
Les États membres prennent les mesures appropriées pour assurer la pleine application des dispositions de la présente directive et déterminent notamment les sanctions à appliquer en cas de violation des dispositions prises en application de la présente directive.

Comme c'est généralement le cas pour une directive, il appartient en premier lieu aux États membres, et non à la Commission, de faire appliquer les dispositions. Par exemple, ce n'est pas à la Commission qu'il incombe de poursuivre ou d'imposer des amendes à ceux qui violent les droits et les obligations prévus dans la directive[18].

2.3. Autres dispositions applicables au spam

Une pratique souvent liée au «spamming» est la récolte (« harvesting ») d'adresses de courrier électronique, c'est-à-dire la collecte automatique de données à caractère personnel sur des lieux publics de l'internet, par ex. le web, les « chatrooms », etc. Cette pratique est illégale en vertu de la directive «générale» 95/46/CE sur la protection des données, que la collecte soit effectuée ou non de manière automatique à l'aide d'un logiciel[19].

Le spam frauduleux et trompeur peut être particulièrement déplaisant. Ces pratiques sont déjà illégales en vertu des règles existantes de l'UE sur la publicité mensongère et les pratiques commerciales déloyales (par exemple, la directive 84/450/CEE sur la publicité mensongère)[20]. Généralement, les lois nationales prévoient aussi des peines plus sévères dans les cas les plus graves, y compris des sanctions pénales.

Des catégories spécifiques de spam peuvent être encore plus choquantes, notamment le spam pornographique ou incluant de la violence gratuite, en particulier lorsque des enfants y sont exposés[21]. Bien que le contenu de certains de ces messages puisse être préjudiciable sans être en soi illégal, leur distribution sans discernement aux enfants aussi bien qu'aux adultes est généralement illégale en vertu du droit interne, et peut parfois être passible de lourdes peines. Il peut arriver que des messages de spam aient un contenu illégal, par exemple une incitation à la haine pour des motifs liés à la race, au sexe, à la religion ou à la nationalité. En tout état de cause, dès que ces messages poursuivent un but de prospection directe – et c'est souvent le cas – ils sont soumis à l'interdiction du spam, comme d'autres catégories de courriels non sollicités.

Il faut aussi faire référence à l'exigence, prévue dans la directive 2000/31/CE relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, («directive sur le commerce électronique»), que la communication commerciale doit être clairement identifiable comme telle (article 6, point a) de la directive

---

18 Cette situation diffère de celle où se trouvent par exemple des agences telles que la Federal Trade Commission des États-Unis.

19 Voir également le document de travail du groupe «article 29» sur la protection des données intitulé «Le respect de la vie privée sur Internet – Une approche européenne intégrée sur la protection des données en ligne» (document n° WP 37 adopté le 21 novembre 2000).

20 Directive 84/450/CEE du Conseil du 10 septembre 1984 relative au rapprochement des dispositions législatives, réglementaires et administratives des États membres en matière de publicité trompeuse. JO L 250 du 19.9.1984, p. 17-20. La Commission a récemment présenté une proposition visant à remplacer et à actualiser cette directive (COM(2003) 356 final).

21 Le 24 septembre 1998, le Conseil a adopté une recommandation concernant le développement de la compétitivité de l'industrie européenne des services audiovisuels et d'information par la promotion de cadres nationaux visant à assurer un niveau comparable et efficace de la protection des mineurs et de la dignité humaine (98/560/CE). Cette recommandation a été le premier instrument juridique adopté au niveau de l'UE en ce qui concerne le contenu des services audiovisuels et d'information qui couvre tous les modes de fourniture, de la radiodiffusion à l'internet.

sur le commerce électronique)[22].

En outre, des actes tels que le piratage ou le vol d'identité sont souvent perpétrés pour faciliter le spam, afin d'envoyer du spam ou d'avoir accès à des bases de données d'adresses ou à des ordinateurs. Une grande partie de ces activités seront couvertes par la décision cadre relative aux attaques visant les systèmes d'information, qui prévoit des sanctions pénales. Cette décision cadre, fondée sur une proposition de la Commission, a fait l'objet d'un accord politique en février 2003 et devrait bientôt être officiellement adoptée[23]. Dans de nombreux États membres, l'accès illicite à un serveur ou à un ordinateur personnel ou leur utilisation abusive constituent déjà un acte délictueux passible de poursuites.

3. MISE EN ŒUVRE ET APPLICATION EFFECTIVES PAR LES ÉTATS MEMBRES ET LES POUVOIRS PUBLICS

Ce chapitre porte sur les actions proposées qui seraient à mettre en œuvre principalement par les gouvernements et les pouvoirs publics, dans des domaines tels que les recours et sanctions, les mécanismes de plainte, les plaintes transfrontalières, la coopération avec les pays tiers et la surveillance.

Toutefois, avant de traiter la question du contrôle de l'application, la Commission remarque qu'un certain nombre d'États membres n'ont pas encore transposé la directive «vie privée et communications électroniques», et notamment les dispositions sur les messages électroniques commerciaux non sollicités, qui font partie d'un nouveau cadre de régulation plus vaste des communications électroniques[24]. Le Parlement européen a récemment exprimé son inquiétude à propos de ce retard[25]. À la suite de l'expiration du délai de transposition de la directive «vie privée et communications électroniques» (31 octobre 2003), la Commission a ouvert, en novembre 2003, des procédures d'infraction à l'encontre de plusieurs États membres pour défaut de notification des mesures de transposition[26].

---

22 Directive du Parlement européen et du Conseil du 8 juin 2000, JO L 178 du 17.7.2000. En règle générale, les «communications commerciales» doivent se conformer aux règles qui leur sont applicables dans l'État membre d'établissement du fournisseur de services. Cette règle ne s'applique cependant pas au caractère licite des communications non sollicitées par courrier électronique (voir l'article 3 de la directive sur le commerce électronique et son annexe). Dans les cas (limités) où des personnes physiques ne seraient pas protégées contre les communications commerciales non sollicitées par la directive 2002/58/CE (par exemple s'il ne s'agit pas d'abonnés), les États membres doivent également veiller, en vertu de la directive sur le commerce électronique, à ce que les fournisseurs de services qui effectuent des communications commerciales non sollicitées par courrier électronique consultent régulièrement les registres «opt-out» dans lesquels les personnes physiques qui ne souhaitent pas recevoir ce type de communications peuvent s'inscrire, et respectent le souhait de ces dernières (voir l'article 7 de la directive sur le commerce électronique).

23 Proposition de décision-cadre du Conseil relative aux attaques visant les systèmes d'information, COM(2002) 173 final du 19.4.2002.

24 Voir également le 9e rapport sur la mise en œuvre de la réglementation de l'UE en matière de communications électroniques, disponible à l'adresse URL suivante: http://europa.eu.int/information_society/topics/ecomm/all_about/implementation_enforcement/annualreports/9threport/index_en.htm

25 La Commission a souligné l'importance de mettre en œuvre pleinement, efficacement et ponctuellement le nouveau cadre réglementaire des communications électroniques, y compris la directive «vie privée et communications électroniques», dans sa communication intitulée «Communications électroniques: vers une économie de la connaissance» (COM(2003) 65 du 11 février 2003).

26 Les lettres de mise en demeure ont été envoyées le 25 novembre 2003 (Voir IP/03/1663).

3.1. Introduction

Même si la législation empêchera l'émission d'une certaine quantité de spam, elle ne sera pas suffisante à elle seule. Une application efficace du régime «opt-in» doit être une priorité dans tous les États membres. En plus d'effectifs et de ressources suffisants, cela implique des mécanismes d'application appropriés, y compris transfrontaliers. La coopération avec les pays non membres de l'UE est également capitale. La surveillance est aussi importante, ne serait-ce que pour déterminer les priorités sur lesquelles axer l'application.

Un certain nombre de facteurs semblent influencer l'efficacité des mécanismes d'application:

– la possibilité de faire appliquer la législation au moyen d'amendes ou d'autres sanctions efficaces. Certaines autorités de régulation manquent apparemment toujours de pouvoirs coercitifs (réels);

– la nature des mécanismes de dépôt de plainte et des recours à la disposition des personnes physiques et des sociétés;

– le besoin de clarté et de coordination entre les autorités nationales, étant donné que leurs fonctions se chevauchent parfois dans ce domaine;

– le niveau de sensibilisation des utilisateurs à leurs droits et à la manière de les faire respecter. Il faut indiquer aux utilisateurs où ils doivent porter plainte, les faits qui feront l'objet d'enquêtes ou non, les types d'actions répressives qui peuvent être engagées, et les informations qu'ils doivent fournir aux autorités pour déclencher une enquête;

– la coordination et la coopération entre les États membres et entre les États membres et les pays tiers sur le droit national applicable dans des affaires précises;

– les ressources disponibles pour dépister les expéditeurs de spam actifs dans l'UE ou à l'étranger et qui masquent leur identité, notamment en se servant de l'identité, des adresses ou des serveurs d'autres utilisateurs.

Les mesures applicables pour faire respecter les dispositions relatives aux communications non sollicitées ont été décrites au point 2.2 ci-dessus. Jusqu'à présent, les procédures relatives aux messages électroniques commerciaux non sollicités ont été organisées et gérées d'une manière très disparate[27]. Même si le choix d'une directive comme instrument implique que les États membres aient une certaine marge de manœuvre dans la mise en œuvre de ses dispositions, une application effective est exigée, quelle que soit la méthode utilisée.

Diversité dans les États membres

L'autorité chargée de faire appliquer les dispositions relatives aux communications commerciales non sollicitées n'est pas la même dans tous les États membres. Dans la majorité des cas, c'est l'autorité responsable de la protection des données qui assume la responsabilité à titre principal. Dans certains pays toutefois, c'est l'autorité de régulation nationale des communications électroniques (ARN) qui remplit cette mission. Dans d'autres pays encore, l'application des règles incombe principalement aux autorités responsables de la protection des consommateurs (y compris l'ombudsman des consommateurs). Il est fréquent que plusieurs autorités doivent être associées à l'exécution des dispositions relatives aux communications non sollicitées. De plus, le spam implique dans de nombreux cas des pratiques trompeuses ou frauduleuses. (Une minorité d'États membres n'ont pas d'autorité de protection des consommateurs et

[27] Il faut noter que les plaintes portent souvent aussi sur des aspects connexes, comme le droit d'accès aux données à caractère personnel et le droit de s'opposer à un traitement de ces données.

l'application des règles est laissée aux associations de consommateurs ou aux consommateurs eux-mêmes.) Les activités de spamming sont souvent liées à des infractions aux règles sur la protection des données telles que la collecte d'adresses électroniques, sinon à des activités de cybercriminalité comme l'intrusion illicite dans des PC ou des serveurs. Ce ne sont pas nécessairement les mêmes autorités qui sont chargées de faire appliquer les dispositions en la matière, a fortiori à une échelle transfrontalière.

Sauf dans un petit nombre d'États membres, une plainte ne débouche pas nécessairement sur une enquête. On a parfois recours à des contacts «pré-infraction», incluant des consignes et des orientations données aux entreprises, avec quelque succès. Parfois, cette phase préalable à la plainte est laissée au consommateur, à qui il appartient de contacter la société concernée avant d'introduire une plainte. Certains pays comme le Royaume-Uni ont recours à l'autorégulation pour organiser cette première phase d'action. Dans certains États membres, il existe déjà des mécanismes de dépôt de plainte dans le cadre d'une autorégulation. Il est fréquent aussi que les autorités agissent de leur propre initiative. Le fait qu'une autorité administrative soit spécialement chargée de ces questions n'exclut pas, en principe, l'accès direct au système judiciaire.

Toutes les autorités chargées de la protection des données n'ont pas le pouvoir d'agir à l'encontre de personnes morales. Toutes n'ont pas non plus (jusqu'ici) la possibilité d'imposer des sanctions. Elles doivent pour ce faire lancer une procédure auprès des autorités judiciaires. En France, l'expérience de la «boîte à spam» a conduit l'autorité responsable de la protection des données à sélectionner quelques affaires et à les porter en justice, sans beaucoup de succès. En Belgique, une expérience analogue a conduit à un échange de vues avec les émetteurs suspectés; dans les affaires transfrontalières, on les a renvoyés aux autorités correspondantes d'autres États de l'UE, ou à la FTC des États-Unis.

Une approche équilibrée comprenant un volet législatif, le contrôle de l'application des règles et une autorégulation est souvent décrite comme le moyen le plus efficace pour faire appliquer le régime «opt-in». Les États membres sont invités à évaluer l'efficacité de leur mécanisme d'application, notamment sur la base des diverses actions proposées ci-dessous (voir les points 3.2 à 3.6).

Les États membres sont également invités à développer des stratégies nationales pour assurer la coopération entre les autorités responsables de la protection des données, les autorités chargées de la protection des consommateurs et les autorités de régulation nationales pour les communications électroniques (ARN), et à éviter le chevauchement de compétences et les doubles emplois entre les différentes autorités.

Pour faciliter et coordonner les échanges d'informations et les meilleures pratiques en matière d'application efficace (par exemple en ce qui concerne les plaintes, les recours, les sanctions, la coopération internationale), les services de la Commission ont créé un **groupe en ligne informel sur les communications commerciales non sollicitées**, avec l'appui des États membres et des autorités responsables de la protection des données. Ce groupe facilitera et coordonnera également le travail sur les autres actions répertoriées dans la présente communication, telles que la sensibilisation et les solutions techniques.

Les documents rédigés à la suite de discussions du groupe seront en général soumis, en vue d'une action appropriée, au Comité des communications (COCOM) créé en vertu du cadre réglementaire des réseaux et services de communications électroniques, et/ou au groupe de travail «article 29» sur la protection des données. Le groupe peut notamment élaborer des critères d'évaluation comparative pour les différentes mesures à proposer.

Ce groupe en ligne comprend des représentants des administrations nationales compétentes et des autorités chargées de la protection des données, ainsi que des services de la Commission. Le groupe en ligne déterminera comment assurer la participation d'autres parties concernées.

3.2. Voies de recours et sanctions efficaces

3.2.1. Discussion

Actuellement, les recours comprennent généralement des amendes ou une «injonction de mettre fin» au traitement illégal des données, accompagnée de temps en temps du «blocage» des sites web impliqués. Dans certains États membres, l'injonction de mettre fin au traitement précède ou accompagne l'imposition d'amendes en cas de non-respect. Néanmoins, toutes les autorités ne sont pas compétentes pour traiter l'ensemble des infractions relatives au spam, et elles n'ont pas toutes les mêmes outils à leur disposition. Il est fréquent que des affaires soient renvoyées devant les autorités judiciaires. Par ailleurs, tous les États membres n'ont pas prévu de sanctions judiciaires pour les infractions concernées.

Tous les États membres ne prévoient pas de voies de recours et d'amendes/sanctions dans leur droit administratif ou pénal. Les sanctions pénales varient d'un État membre à l'autre et incluent parfois des peines de prison. De plus, il est généralement possible de réclamer des dommages et intérêts en vertu du droit civil.

Il existe souvent une distinction entre infractions légères et infractions graves (par ex. multipostage massif, publicité et pratiques commerciales trompeuses ou frauduleuses), et les sanctions elles-mêmes varient fortement d'un État membre à l'autre.

Dans de nombreux cas, les activités de spam peuvent aussi ouvrir les voies de droit prévues par la législation générale sur la protection des données (par exemple, violation de l'obligation de notifier, du droit d'accès, de l'obligation de nommer un représentant dans un État membre de l'UE, etc.) ou en vertu d'une législation spécifique (sur la publicité mensongère, les pratiques commerciales frauduleuses, etc.). Avant l'introduction du régime «opt-in», divers arguments juridiques ont été utilisés pour s'attaquer à certaines formes de spam (les campagnes de multipostage, l'utilisation illégitime de données à caractère personnel, la perturbation d'un réseau, l'abus de compte de courrier électronique, la fraude et l'interprétation erronée d'un contrat, par exemple).

D'une façon générale, le recours juridictionnel n'est pas considéré comme un mécanisme d'application suffisant. Des amendes administratives peuvent généralement être imposées par l'autorité responsable de la protection des données, l'autorité chargée de la protection des consommateurs et/ou l'ARN, mais leurs montants varient. Les États membres qui n'ont pas cette possibilité actuellement envisagent en général son introduction. Comparées aux solutions judiciaires, les sanctions administratives semblent être particulièrement adaptées à ce secteur dynamique. Les autorités responsables de la protection des données, de la protection des consommateurs, ainsi que les ARN, se servent souvent elles-mêmes d'instruments complémentaires pour faire appliquer la réglementation. Les procédures administratives peuvent s'avérer à la fois peu coûteuses et rapides.

3.2.2. Actions proposées

Comme condition préalable, la Commission invite les États membres qui n'ont pas encore transposé la directive, et notamment ses dispositions relatives aux communications non sollicitées, à achever cette tâche sans retard supplémentaire. Les services de la Commission sont disposés à aider les États membres en cas de besoin.

Les États membres sont invités à évaluer l'efficacité de leur système de recours et de sanctions appliquées en cas d'infraction, et à donner aux victimes des possibilités adéquates de réclamer des dommages et intérêts.

Les États membres et les autorités compétentes qui n'ont pas de voie de recours administratif devraient envisager de se doter de ce type de recours contre le spam, afin de disposer d'une procédure rapide, peu coûteuse et efficace pour faire appliquer le régime «opt-in».

La Commission vérifiera que les mesures de transposition nationales prévoient bien des sanctions réelles en cas de non-respect des exigences applicables par les acteurs du marché, y compris le cas échéant des sanctions financières et pénales.

Dans ce contexte, la Commission examinera également dans quelle mesure les autorités compétentes disposent des pouvoirs d'investigation et d'exécution nécessaires.

3.3. Mécanismes de plainte

3.3.1. Discussion

Une application efficace des règles implique des mécanismes de plainte appropriés. Certaines autorités responsables de la protection des données ont créé des boîtes de courrier électronique auxquelles les utilisateurs peuvent transmettre les courriels commerciaux non sollicités, et se sont engagées à intervenir dans des cas déterminés.

Certains États membres semblent préférer des procédures administratives normales et/ou la prise de contact avec les ISP ou avec les équipes d'intervention en cas d'urgence informatique (CERT) s'il y a perturbation de réseau. D'autres États membres favorisent des procédures plus traditionnelles (action en dommages-intérêts dans le cadre du droit civil/procédures administratives). La corégulation ou l'autorégulation sont parfois citées comme des solutions préférables aux mesures d'exécution directe.

Meilleures pratiques

Fin 2002, la France et la Belgique ont mis en place des boîtes de courrier électronique pour recevoir des plaintes précises relatives au spam, et les résultats sont tout à fait intéressants. Des rapports sur ces initiatives sont à la disposition du public[28]. La France devrait adopter ce système de boîte électronique sur une base permanente dans le cadre des nouvelles règles transposant la directive «vie privée et communications électroniques». La « Federal Trade Commission » (FTC) aux États-Unis exploite une boîte électronique du même type et utilise les messages entrants comme base pour engager des poursuites sur la base de la législation existante sur les pratiques commerciales déloyales et trompeuses[29].

L'un des avantages des boîtes aux lettres électroniques est qu'elles semblent encourager les consommateurs à dénoncer les infractions et contribuent donc à rendre plus efficace l'application de la législation adoptée. Elles peuvent en outre fournir des statistiques essentielles sur l'ampleur et la nature des problèmes rencontrés dans un pays ou une région, donnant ainsi une vue d'ensemble claire qui constitue pour les autorités un outil précieux pour fixer ou adapter les priorités en matière d'application. De plus, des actions préventives peuvent être mises au point sur la base des connaissances acquises. Ainsi, la CNIL (l'autorité française chargée de la protection des données) a utilisé des informations recueillies au cours

---

28 Le rapport du 24 octobre 2002 adopté par la Commission nationale Informatique et Libertés (CNIL), l'autorité française responsable de la protection des données, est disponible à l'adresse URL suivante: http://www.cnil.fr/frame.htm?http://www.cnil.fr/thematic/internet/spam/spam_sommaire.htm
Le rapport adopté en juillet 2003 par la Commission de protection de la vie privée, l'autorité belge chargée de la protection des données, peut être consulté à l'adresse URL suivante: http://www.privacy.fgov.be/publications/spam_4-7-03_fr.pdf.

29 Voir par exemple http://www.ftc.gov/bcp/conline/pubs/online/inbox.pdf. Les messages non sollicités ou trompeurs peuvent être envoyés à l'adresse suivante: uce@ftc.gov.

de son opération «boîte à spams» pour élaborer des dossiers d'information préventive destinés aux utilisateurs et aux responsables du marketing.

L'utilité d'une boîte aux lettres électronique pour surveiller et mesurer l'ampleur et le champ d'application du spam dépend naturellement de la capacité d'enquêter utilement et rapidement sur les plaintes déposées.

Seuls certains États membres semblent envisager la possibilité d'utiliser eux-mêmes une boîte aux lettres électronique spécialisée, alors qu'il existe de manière générale un intérêt pour l'expérience acquise par d'autres États membres grâce à cette méthode. Les raisons indiquées sont généralement: la possibilité existante d'introduire une plainte par courrier électronique, en général par l'intermédiaire du site web de l'autorité; la nécessité de disposer de personnel spécialisé et d'équipement supplémentaires, ou encore la nécessité de modifier des procédures juridiques existantes.

3.3.2. Actions proposées

Les États membres et les autorités compétentes devraient évaluer l'efficacité de leur système juridique pour traiter les plaintes des utilisateurs et envisager des adaptations le cas échéant.

Les États membres et les autorités compétentes sont invités à mettre en place des boîtes aux lettres électroniques spécialisées, dont le lancement sera soutenu par des campagnes d'information.

Ces boîtes aux lettres spécialisées devraient être conçues de manière à permettre des recherches simples et des analyses visant à mieux comprendre le problème et à fixer des priorités pour l'application de la législation.

Les services de la Commission faciliteront le partage d'informations sur les expériences de boîtes aux lettres électroniques.

3.4. Plaintes transfrontalières et coopération en matière d'application à l'intérieur de l'UE

3.4.1. Discussion

Le traitement efficace des plaintes transfrontalières est une des opérations qui permettent d'assurer avec succès la protection des consommateurs dans ce secteur. En tout état de cause, il sera primordial de relier les mécanismes de plaintes nationaux, quelles que soient leurs modalités, de manière que les plaintes formées par des utilisateurs dans un État membre concernant des messages en provenance d'un autre État membre soient, elles aussi, traitées avec efficacité (voir le paragraphe 3.5 ci-dessous pour la coopération avec les pays tiers).

Actuellement, tous les États membres ne disposent pas d'une procédure formelle pour traiter des plaintes transfrontalières. Parmi les solutions actuellement utilisées, on peut citer la prise de contacts avec l'autorité compétente dans un autre État membre et la possibilité de transférer la plainte à l'autorité compétente de l'État d'origine du (des) message(s).

Au niveau européen, les autorités chargées de la protection des données (y compris celles de l'EEE et des pays candidats) s'efforcent de procéder à des échanges d'informations sur les plaintes transfrontalières par l'intermédiaire d'un «atelier sur le traitement des plaintes» (« complaints handling workshop »), créé dans le cadre de la conférence européenne des commissaires chargés de la protection des données. Il est possible d'y avoir recours pour les

plaintes transfrontalières relatives au spam et notamment pour déterminer la législation applicable dans des cas bien précis. Dans le même temps, il faut savoir que ce ne sont pas toujours les autorités chargées de la protection des données qui appliquent les dispositions sur les communications non sollicitées.

Dans le domaine de la protection des consommateurs, la Commission a récemment proposé un règlement relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs pour traiter des problèmes transfrontaliers[30]. Il met en place des procédures d'assistance mutuelle et prévoit une coopération opérationnelle approfondie entre les autorités nationales. Les spams qui sont mensongers ou trompeurs ou qui enfreignent d'autres règles dans le domaine de la protection des consommateurs seraient couverts par le régime proposé, mais pas tous les spams interdits par la directive concernant la vie privée et les communications électroniques. Ce règlement est actuellement examiné par le Conseil et le Parlement.

[30] COM(2003) 443 final.

3.4.2. Actions proposées

Les États membres et les autorités compétentes sont invités à évaluer l'efficacité de leurs procédures existantes en matière de traitement des plaintes transfrontalières (accords d'assistance mutuelle, par exemple).

La coordination des actions entre les administrations nationales compétentes est encouragée. Il peut s'agir, notamment, d'activités de coordination et d'échange d'informations entre les autorités chargées de l'application des nouvelles dispositions, et entre ces dernières et d'autres autorités responsables de formes particulières de spam (par exemple, les spams frauduleux ou «scams», les spams pornographiques, les messages sur les produits de santé illégalement distribués).

En ce qui concerne les spams frauduleux et trompeurs, le Conseil et le Parlement sont invités à approuver le règlement proposé sur la coopération en matière de protection des consommateurs aussi rapidement que possible pour faire en sorte que les autorités de l'UE chargées de la protection des consommateurs disposent de tous les outils nécessaires pour traiter les spams mensongers et trompeurs. Ils sont également invités à examiner la possibilité d'étendre le champ d'application de ce règlement à la directive concernant la vie privée et les communications électroniques.

Les États membres sont invités à étudier les moyens de supprimer les obstacles existants à l'échange d'informations et à la coopération ainsi que la possibilité de demander à leur homologues dans d'autres États membres de prendre des mesures. Dans la pratique, il pourrait être utile de disposer d'un mécanisme de liaison (voir l'initiative précitée des autorités chargées de la protection des données) dans le cadre duquel les régulateurs nationaux pourraient coopérer à la mise en œuvre transfrontalière. L'établissement d'un réseau de soutien à la coopération pourrait se fonder sur des programmes existants de la Commission tels qu'IDA[31].

La Commission entend faciliter et promouvoir ces efforts de coordination entre les autorités nationales compétentes, notamment par l'intermédiaire du groupe en ligne informel sur les communications commerciales non sollicitées qui vient d'être créé. Les services de la Commission ont commencé à examiner, avec l'aide des États membres et des autorités nationales concernées par la mise en œuvre, le type d'action concrète qui serait nécessaire pour améliorer le traitement des plaintes transfrontalières. Les discussions avec les autorités nationales se poursuivront tout au long de l'année 2004.

3.5. Coopération avec les pays tiers

3.5.1. Discussion

Les nouvelles règles s'appliquent au traitement des données à caractère personnel dans le cadre de la fourniture de services de communications électroniques accessibles au public sur les réseaux publics de communications dans l'Union européenne (et dans l'EEE). Par conséquent, l'article 13 de la directive 2002/58/CE établissant la règle du consentement

[31] Des informations sur le programme IDA sont disponibles via l'adresse URL suivante : http://europa.eu.int/comm/enterprise/ida/index.htm

préalable («opt-in») s'applique à toutes les prospections commerciales non sollicitées à destination et en provenance de réseaux se trouvant dans l'Union européenne (et dans l'EEE). Cela signifie que les messages provenant de pays tiers doivent également être conformes aux règles de l'UE, au même titre que les messages provenant de l'UE et envoyés à des destinataires dans des pays tiers.

La mise en œuvre effective des règles en ce qui concerne les messages provenant de pays tiers sera sans aucun doute plus compliquée que pour les messages issus de l'UE. Elle revêt néanmoins une importance capitale puisqu'une bonne partie du spam provient de l'extérieur de l'UE.

Il faudra, pour ce faire, disposer d'une palette d'instruments comportant notamment des mesures de prévention, des dispositifs de filtrage, des mesures d'autorégulation et des dispositions contractuelles et des mesures de coopération internationale. Le présent chapitre est consacré en particulier à la coopération internationale. Le premier objectif de la coopération internationale est de promouvoir l'adoption d'une législation efficace dans les pays tiers. Le deuxième objectif est de coopérer avec les pays tiers pour assurer une mise en œuvre efficace des règles applicables.

On ne dispose pas de beaucoup d'expérience sur la mise en œuvre des règles existantes de consentement préalable (opt-in) ou d'opposition (opt-out) pour les communications provenant de l'extérieur de l'UE. Outre le fait que le spam est un phénomène relativement nouveau, on cite le plus souvent, Au nombre des obstacles à cette mise en œuvre, la difficulté d'identifier les expéditeurs de ce spam ou les efforts nécessaires pour y parvenir; le manque de mécanismes internationaux (appropriés) de coopération; et l'absence de compétence de certaines autorités sur les questions internationales.

En ce qui concerne le spam frauduleux et trompeur, la proposition de règlement de la Commission sur la coopération en matière de protection des consommateurs prévoit également des dispositions en matière de coopération avec les pays tiers sur la mise en œuvre des règles. L'Organisation de coopération et de développement économiques (OCDE) a adopté en 2003 une recommandation visant à protéger les consommateurs contre les pratiques commerciales transfrontalières frauduleuses et trompeuses[32].

3.5.2. Actions proposées

Au niveau multilatéral, certains États membres participent déjà activement à des forums tels que l'OCDE, où des travaux sur le spam ont commencé. Une participation active à ces travaux est encouragée, notamment en ce qui concerne l'élaboration de solutions au niveau international.

La Commission accueillera, en février 2004, un atelier de l'OCDE sur le spam qui vise à faire mieux comprendre les problèmes que pose le spam et à contribuer à l'élaboration de solutions au niveau international. Des actions de suivi concrètes seront engagées au niveau de l'OCDE sur la base des résultats de l'atelier. Les services de la Commission examinent ces actions de suivi avec les États membres, ainsi que les travaux entrepris par l'OCDE pour promouvoir une législation internationale efficace, la sensibilisation, les solutions techniques, l'autorégulation, et la coopération internationale dans le domaine de la mise en œuvre.

[32] Lignes directrices de l'OCDE régissant la protection des consommateurs contre les pratiques commerciales transfrontières frauduleuses et trompeuses, OCDE, 2003.

En ce qui concerne les Nations-Unies, la déclaration de principe du sommet mondial sur la société de l'information (Genève, 10-12 décembre 2003) et le Plan d'action qui lui est associé soulignent que le spam devrait être traité aux niveaux nationaux et internationaux appropriés. La Commission s'efforcera de déterminer les meilleurs moyens d'assurer le suivi des résultats du sommet mondial dans l'UE en prévision de la phase de Tunis qui aura lieu en 2005.

Les États membres et les autorités compétentes sont également invités à renforcer la coopération bilatérale avec les pays tiers, ou à mettre en place des activités de ce type si elles n'existent pas encore. Cela comprend non seulement la promotion d'une législation efficace mais également la coopération dans le domaine de la mise en œuvre, y compris, le cas échéant, la coopération policière et judiciaire.

La coopération est également encouragée entre les autorités et le secteur privé, notamment les ISP et les ESP, afin de remonter jusqu'aux expéditeurs de spam, sous réserve des garanties juridiques appropriées.

Les services de la Commission continueront à participer activement aux travaux qui se déroulent dans les enceintes internationales, notamment à l'OCDE et dans le cadre de l'atelier que la Commission accueillera à Bruxelles en février 2004. Elle continuera également à organiser des réunions et des discussions bilatérales avec les pays tiers, notamment pour encourager les pays tiers à prendre des mesures efficaces contre le spam, en particulier sous ses formes les plus offensives, et à promouvoir la coopération sur la mise en œuvre.

Les services de la Commission ont commencé à examiner, avec l'aide des États membres et des autorités nationales concernées par la mise en œuvre, le meilleur moyen de garantir une coopération internationale, notamment en ce qui concerne le traitement des plaintes concernant le spam provenant de pays tiers. Ces travaux avec les autorités nationales se poursuivront tout au long de l'année 2004.

3.6. Monitoring

3.6.1. Discussion

Afin d'évaluer le fonctionnement pratique du système de consentement préalable et de traiter des problèmes donnés avec les mesures appropriées, les États membres auront besoin d'informations objectives et à jour sur les tendances en matière de spam, de plaintes des utilisateurs et de difficultés rencontrées par les fournisseurs de services. Les sources et le type d'informations nécessaires à cette fin pourraient comprendre les tendances concernant la nature de spam, l'origine et le volume de courrier électronique commercial non sollicité détecté par un filtrage des fournisseurs de logiciel, des fournisseurs de services et des initiatives (réglementaires) nationales et, le cas échéant, les statistiques provenant des plaintes par voie de boîtes aux lettres électroniques.

L'OCDE a commencé à travailler en 2003 sur la mesure des messages électroniques non sollicités au niveau international et va poursuivre ses travaux en 2004.

L'article 18 de la directive concernant la vie privée et les communications électroniques prévoit, pour 2006, un rapport sur l'application de la directive et sur son impact sur les opérateurs économiques et les consommateurs, notamment en ce qui concerne les dispositions relatives aux communications non sollicitées. Pour élaborer ce rapport, la Commission devra obtenir des informations auprès des États membres, et notamment des statistiques appropriées.

3.6.2. Actions proposées

Les États membres devraient faire en sorte de disposer des informations et des statistiques nécessaires pour cibler leurs efforts dans le domaine de la mise en œuvre, le cas échéant en coopération avec l'industrie et en tenant compte des travaux en cours à l'OCDE sur la mesure des messages électroniques non sollicités.

La Commission fera appel au groupe en ligne informel nouvellement créé sur les communications commerciales non sollicitées pour faciliter et coordonner les échanges d'informations et les meilleures pratiques sur les tendances et les statistiques en matière de spam.

4. ACTIONS TECHNIQUES ET ACTIONS D'AUTOREGULATION POUR L'INDUSTRIE

Le présent chapitre relatif à l'autorégulation et aux questions techniques couvre les mesures concernant surtout les acteurs du marché, dans des domaines tels que les dispositions contractuelles, les codes de conduite, les pratiques de marketing acceptables, les labels, les formules substitutives de règlement des différents, ainsi que certaines solutions techniques comme le filtrage et la sécurité des serveurs.

4.1. Application efficace du régime «opt-in»

4.1.1. Discussion

La lutte contre les communications commerciales non sollicitées est l'affaire de toutes les parties concernées. L'industrie peut jouer un rôle spécifique dans ce cadre en faisant du régime «opt-in» une pratique commerciale quotidienne. La pratique quotidienne recouvre non seulement les conditions appliquées aux utilisateurs finals, mais aussi les rapports avec les partenaires commerciaux.

Dans bien des cas, il convient de garantir une coordination plus étroite au travers des associations professionnelles et une meilleure participation des organes d'autorégulation sectoriels et des associations de consommateurs/utilisateurs, ainsi que des autorités responsables de la protection des données ou d'autres autorités nationales compétentes.

Meilleures pratiques

Ainsi, aux Pays-Bas, l'«Electronic Commerce Platform» héberge depuis 2002 une plateforme consacrée aux principes fondamentaux des communications électroniques commerciales, qui regroupe diverses branches du secteur (entreprises de prospection directe et ISP) et l'association hollandaise des consommateurs. Cette initiative a pour objectif de développer la mise en œuvre pratique du principe «opt-in». Cette mise en œuvre pratique sera évaluée par l'autorité responsable de la protection des données[33].

Les contrats peuvent contribuer à la lutte contre le spam, lorsqu'ils sont assortis de clauses de sauvegarde protégeant les droits individuels. Bon nombre de fournisseurs de services internet (ISP) et de fournisseurs de services de courrier électronique (ESP) font d'ores et déjà figurer dans les contrats qu'ils passent avec leurs clients des obligations visant notamment à interdire l'utilisation de leurs services pour l'envoi de spam. Ces ISP et ESP interdisent déjà l'envoi de

[33] Voir http://www.ecp.nl/projecten.php#32.

courrier électronique non sollicité et le multipostage à partir de leurs comptes de courrier électronique[34].

Il est fort probable que les concepts utilisés jusqu'ici dans les contrats conclus entre les ISP et leurs clients soient différents de ceux utilisés dans la nouvelle directive et dans la législation nationale de la transposition.

En termes de service clientèle, il importe également d'adopter une politique de filtrage plus volontariste en communiquant aux utilisateurs des informations sur les filtres anti-spam et en proposant en option aux abonnés des services ou des dispositifs de filtrage.

Il en va de même lorsque les ISP ou les opérateurs de réseaux mobiles passent des contrats avec des tiers, et notamment avec des sociétés de vente directe. Sont concernées non seulement les relations directes avec les entreprises proposant des services à «valeur ajoutée», mais également les situations dans lesquelles un prestataire de services donné a conclu avec des opérateurs des accords d'interconnexion, comme c'est le cas pour les services mobiles.

Le nouveau régime «opt-in» a également des répercussions sur plusieurs activités de prospection directe, telles que:

- les méthodes utilisées pour la collecte d'adresses électroniques et d'autres coordonnées électroniques conformément au nouveau régime (comme indiqué plus haut, la collecte d'adresses courriel est contraire au droit communautaire);

- l'adaptation des listes existantes;

- les interdictions frappant l'utilisation des données sans consentement et la vente de listes non-conformes à la réglementation.

4.1.2. Actions proposées

Il convient de promouvoir la participation de l'industrie et l'autorégulation, voire la corégulation, notamment dans les domaines où la législation et les mesures d'application des pouvoirs publics risquent de se révéler insuffisantes. Toutes les parties concernées ont leur rôle à jouer, y compris les associations de consommateurs et/ou d'utilisateurs.

Pratiques contractuelles des fournisseurs de services envers leurs abonnés et partenaires commerciaux

Premièrement, l'industrie devra en particulier évaluer la conformité des contrats existants aux nouvelles dispositions et procéder, le cas échéant, aux adaptations qui s'imposent.

Il s'agira d'adapter les conditions figurant dans les contrats d'abonné. Sont concernés non seulement les ISP et les ESP, mais également les fournisseurs de services mobiles. Les acteurs concernés pourraient, à titre complémentaire, informer leurs clients sur les filtres et les logiciels ou services de filtrage, et les leur proposer en option dans le cadre du service clientèle (pour le filtrage, voir également le point 4.3 ci-dessous). Les clauses figurant dans les contrats passés avec les partenaires commerciaux (dans le cas, par exemple, de

[34] Ces dispositions reposent parfois sur la nécessité de prendre toutes les mesures nécessaires pour prévenir une utilisation inopportune des services. Dans d'autres cas, les dispositions font référence à des codes de conduite existants concernant le multipostage ou à des principes d'autorégulation (par exemple la "Netiquette").

l'interconnexion mobile et des services à valeur ajoutée) devraient également correspondre à des pratiques commerciales conformes au régime «opt-in» et prévoir des sanctions appropriées en cas d'infraction.

Pratiques des sociétés de marketing direct

Deuxièmement, les sociétés de marketing direct pourraient devoir adapter leurs pratiques au régime «opt-in». Elles pourraient notamment s'entendre sur des méthodes spécifiques et licites de collecte des données personnelles (comme les systèmes à inclusion confirmée ou « double opt-in » on « confirmed opt-in»).

Codes de conduite

Troisièmement, les associations sectorielles ont déjà annoncé diverses initiatives, telles que l'adaptation ou l'adoption de codes de conduite et la diffusion de bonnes pratiques de prospection commerciale[35]. La Commission soutiendra l'élaboration de codes de conduite en ligne à l'échelle européenne dans le domaine de la prospection directe. Les codes de conduite et autres initiatives d'autorégulation et les contrats doivent être conformes aux règles du régime «opt-in». La participation de l'autorité réglementaire compétente pourrait être utile à cet égard. Il convient de rappeler dans ce contexte que le groupe de travail «article 29» sur la protection des données peut approuver des codes de conduite au niveau de l'UE (voir l'article 30 de la directive 95/46/CE, qui est la directive «générale» en matière de protection des données).

Comme c'est souvent le cas, l'application effective des solutions reposant sur l'autorégulation dépendra de la structure qui sera mise en place pour contrôler la conformité aux règles convenues, et notamment de l'efficacité des sanctions prévues.

Labels

Quatrièmement, la sensibilisation des utilisateurs pourrait être assurée au moyen d'instruments tels que des labels (« trusmarks », « webseals), notamment lorsque le respect des codes de conduite par les acteurs du marché est supervisé et certifié par des tierces parties de confiance.

La présence de labels visibles peut aider les utilisateurs à identifier les ISP, les ESP et les autres acteurs industriels qui se conforment aux règles de l'UE et/ou à des codes de conduite reconnus mettant en œuvre ces règles. Ces labels pourraient également contribuer à renforcer l'efficacité des systèmes de filtrage.

On pourrait envisager de munir de tels labels les bases de données utilisateurs et les messages électroniques qui respectent le régime «opt-in» (par exemple, apposition du label «ADV» dans la ligne de sujet d'un message électronique pour indiquer qu'il contient de la publicité).

Les labels pourraient également permettre aux destinataires d'identifier clairement ces communications commerciales conformément à la directive concernant le commerce électronique (voir l'article 6 (a) de la directive 2000/31/CE, ainsi que le point 2 ci-dessus).

[35] La Fédération européenne de marketing direct (FEDMA) a annoncé la publication en ligne d'un code de conduite destiné aux sociétés de prospection directe.

4.2. Systèmes alternatifs de règlement des conflits (ADR)

4.2.1. Discussion

Dans le cas d'atteintes à la vie privée telles que l'envoi de communications commerciales non sollicitées, la mise en place d'un mécanisme extrajudiciaire de règlement des litiges pourrait permettre de mieux faire respecter les nouvelles règles. Différentes initiatives ont été lancées au niveau national et au niveau de l'UE afin de créer des mécanismes alternatifs de règlement des conflits (ADR) pour les litiges en rapport avec les transactions et communications en ligne. La Commission a adopté en 1998 et en 2001 des recommandations relatives à l'ADR dans lesquelles sont établis les principes applicables à ces systèmes. Plusieurs initiatives ont été lancées dans le domaine des systèmes d'ADR axés sur la protection des consommateurs (par exemple le réseau extrajudiciaire européen EEJ-NET)[36]. L'article 17 de la directive sur le commerce électronique encourage également le développement de tels mécanismes.

Il existe dans certains pays des mécanismes extrajudiciaires de règlement des litiges. Parfois institués au titre de la législation, ces mécanismes diffèrent les uns des autres à de nombreux égards, tels que l'origine (mécanismes sectoriels, par exemple la prospection directe ou la prospection par courrier électronique), la compétence, les pouvoirs et les sanctions (par exemple dommages-intérêts), la participation d'autorités spécifiques (par exemple les autorités chargées de la protection des données, les organismes de déontologie publicitaire), etc.

Pour être efficaces, ces mécanismes doivent satisfaire à certaines conditions ayant trait notamment à leur organisation et à leur promotion, ainsi qu'aux mesures prises en vue de garantir l'exécution de leurs décisions. Leur mise en place exigerait également une coopération entre les pouvoirs publics et l'industrie.

4.2.2. Actions proposées

Il serait souhaitable que soient créés, sur la base, dans toute la mesure du possible, des initiatives existantes (comme le réseau extrajudidiaire européen EEJ-NET), des mécanismes efficaces de plainte fondés sur l'autorégulation et des mécanismes substitutifs de règlement des différends (ADR). La création de tels mécanismes pourrait se révéler particulièrement utile dans les cas où la coopération internationale est plus difficile à réaliser.

4.3. Questions techniques

4.3.1. Discussion

Différentes solutions sont utilisées pour lutter contre le spam sur le plan technique. La communauté internet (RIPE, IETF, etc.) prend elle aussi très au sérieux le problème du spam[37]. Les initiatives à plus long terme, comme les nouvelles normes techniques applicables au courrier électronique, ne sont pas couvertes dans le présent document. Les ISP et les ESP bloquent souvent les messages provenant de serveurs utilisés pour l'envoi de communications commerciales non sollicitées (courrier électronique) jusqu'à ce que la source du spam soit

---

36 Pour de plus amples renseignements, voir : http://europa.eu.int/comm/consumers/redress/out_of_court/index_en.htm.

37 Ainsi, le groupe de travail RIPE (Réseaux IP Européens) sur la lutte contre le spam mène depuis 1998 des actions dans ce domaine (voir le document intitulé "Good Practice for combating Unsolicited Bulk Email" (bonnes pratiques en matière de lutte contre le multipostage non sollicité) qui figure sur le site RIPE (voir: http://www.ripe.net). Plus récemment, l'IRTF (Internet Research Task Force) a créé un groupe de recherche sur la lutte contre le spam (voir: http://www.irtf.org/charters/asrg.html). Ce groupe pourrait mettre au point certaines technologies susceptibles de servir de point de départ aux efforts de normalisation entrepris au sein de l'IETF (Internet Engineering Task Force).

identifiée et que l'utilisation du serveur lui soit interdite. En outre, des logiciels de filtrage peuvent être employés par les utilisateurs sur leur propre équipement terminal ou par les prestataires de services de communications électroniques sur leurs serveurs.

Toutefois, toutes les pratiques et techniques de filtrage n'offrent pas le même degré de contrôle à l'utilisateur. Elles n'offrent pas non plus les mêmes garanties en termes de protection des données et de la vie privée, et notamment de respect de la confidentialité des communications. Il se peut par ailleurs qu'elles ne soient pas encore alignées sur le nouveau régime «opt-in» applicable dans les pays de l'UE en matière de communications commerciales (consentement préalable, prospection commerciale, multipostage et communications individuelles). En outre, l'établissement d'une distinction plus claire entre la prospection commerciale licite (par exemple les pratiques conformes au régime «opt-in») et les communications commerciales non sollicitées pourrait permettre le développement de logiciels de filtrage plus efficaces.

Si les nouvelles dispositions juridiques sur le courrier électronique commercial non sollicité prévoient des garanties supplémentaires pour l'utilisateur et assurent aux fournisseurs de services une plus grande sécurité pour entreprendre, sur demande, une action contre les expéditeurs de spam, il peut arriver que les dispositifs de filtrage bloquent le courrier électronique légitime (on parle alors de «faux positif») ou laissent passer du spam («faux négatifs»). Dans certains cas, cela risque de déboucher sur une situation dans laquelle l'expéditeur ou le destinataire entreprend une action judiciaire contre un ISP/ESP. Certains ISP/ESP proposent donc en option à leurs utilisateurs un service de filtrage et demandent leur accord pour l'activer.

Le recours à des techniques de filtrage pour lutter contre le spam pose d'autres problèmes tels que les rapports entre le filtrage et la liberté d'expression et entre le filtrage et l'obligation contractuelle de transmettre des messages de courrier électronique aux clients de leurs clients à laquelle sont soumis les ISP/ESP, mais ces questions n'entrent pas dans le champ d'application de la présente communication.

Dans les services mobiles, étant donné que l'environnement commercial est différent de celui qui existe pour les services Internet fixes, des solutions différentes peuvent être envisagées. Dans le cas des services mobiles, on applique généralement des frais de livraison par message qui rendent le spam plus coûteux. Néanmoins, certains nouveaux services impliquent une facturation basée sur la recherche, ce qui signifie que le spam augmente les coûts pour le destinataire. En outre, des messages de courrier électronique peuvent désormais être reçus sur des terminaux mobiles. Des filtres et des fonctions de visualisation pourraient alors être fournis aux abonnés pour gérer le spam mobile.

Il faut également accorder une attention particulière aux relais ouverts. Un serveur relais-ouvert est un serveur SMTP qui peut être utilisé pour relayer des messages envoyés par des utilisateurs qui ne sont pas des utilisateurs locaux du serveur. Dans le passé, la plupart des relais étaient ouverts. Toutefois, quand les relais sont ouverts, ils peuvent être utilisés par les expéditeurs de spam pour envoyer des communications non sollicitées assez facilement. Des mesures préventives simples réduiraient les possibilités d'abus dans ce domaine. Cela est également valable pour les serveurs proxy ouverts, qui sont des serveurs exploitant des logiciels permettant une interaction directe avec l'internet.

4.3.2. Actions proposées

Les États membres et les autorités compétentes sont invités à clarifier les conditions juridiques dans lesquelles différents types de logiciels de filtrage peuvent fonctionner dans le pays concerné, y compris sous l'angle du respect de la vie privée.

Les fournisseurs de logiciels de filtrage doivent veiller à ce que leurs systèmes de filtrage soient compatibles avec le régime «opt-in» et d'autres exigences du droit de l'UE, y compris celles liées à la confidentialité des communications.

Les utilisateurs devraient avoir la possibilité de gérer la manière dont le spam entrant est traité, en fonction de leurs besoins. Les fournisseurs de logiciels de filtrage doivent tenir compte des conséquences, pour les utilisateurs, des cas de «faux positif», de «faux négatif», de certaines formes de filtrage fondé sur le contenu, et des problèmes de responsabilité qui risquent d'y être associés.

Les sociétés de filtrage devraient coopérer avec les parties concernées pour développer des techniques de reconnaissance des courriels commerciaux correspondant aux pratiques commerciales acceptées en vertu du droit communautaire, en utilisant par exemple des labels de confidentialité, d'autres types de labels, etc.

Les fournisseurs de services de courrier électronique (et de services mobiles le cas échéant) devraient proposer en option des équipements ou des services de filtrage aux clients qui en font la demande, et les informer sur ceux proposés par des tiers.

Les propriétaires de serveurs de courrier électronique devraient s'assurer que leurs serveurs sont correctement sécurisés et ne se trouvent pas en mode «relais ouvert» (si cela n'est pas justifié). La même remarque vaut pour les serveurs proxy ouverts.

5. ACTIONS DE SENSIBILISATION

Ce chapitre consacré aux questions de sensibilisation couvre les actions proposées dans des domaines tels que la prévention, la sensibilisation des consommateurs et les plaintes.

5.1. Discussion

Les États membres de l'UE devaient avoir transposé le nouveau régime «opt-in» applicable aux messages électroniques non sollicités dans leur droit interne au plus tard pour le 31 octobre 2003. Or, même si cette nouvelle approche a eu un large écho dans la presse, il reste des incertitudes, parmi les acteurs du marché et le grand public, sur ce que signifie en pratique le régime «opt-in»[38].

Cette nouvelle approche repose sur le droit donné à l'utilisateur d'accepter ou de refuser de recevoir des communications commerciales. Cela implique toutefois que l'utilisateur soit au courant des règles de base applicables aux communications non sollicitées et sache où signaler les problèmes.

---

38 On trouvera des informations de fond sur les règles applicables aux communications non sollicitées en vertu de la directive 2002/58/CE à l'adresse URL suivante: http://europa.eu.int/information_society/topics/ecomm/all_about/todays_framework/privacy_protection/index_en.htm#unsolicited.

Meilleures pratiques

L' « Information Commissioner » du Royaume-Uni (qui est l'autorité responsable de la protection des données au Royaume-Uni) a publié, quelques semaines avant l'entrée en vigueur de la nouvelle réglementation mettant en œuvre la directive, un document d'orientation expliquant les nouvelles règles, dont une partie était consacrée à la prospection commerciale par des moyens électroniques. L' « Information Commission »a aussi annoncé que des formulaires de dépôt de plainte seraient disponibles en ligne et dans ses bureaux dès l'entrée en vigueur des règles, en expliquant quelles informations seraient probablement requises[39].

Les utilisateurs doivent aussi comprendre les risques qu'implique la communication de leurs données à caractère personnel via l'internet (par exemple en les laissant sur des sites web ou des forums de discussion Usenet qu'ils visitent) et devraient adapter leur comportement en conséquence.

Enfin, il faut qu'ils sachent quels types de logiciels de filtrage existent sur le marché et ce que les fournisseurs de services et de logiciels (par ex. ISP, ESP) peuvent faire pour eux.

Meilleures pratiques

La «Commission nationale Informatique et Libertés» (CNIL), qui est l'autorité française responsable de la protection des données, a mis en ligne sur son site web un dossier d'information très complet concernant différents aspects du spam: les résultats de sa campagne «boîte à spam» et les affaires dont elle a saisi les autorités judiciaires (voir ci-dessous), des conseils de base sur la prévention du spam, des informations sur la manière de signaler le spam, les coordonnées des associations d'utilisateurs actives dans ce domaine, etc.

Bien que des activités de sensibilisation concernant le nouveau régime «opt-in» aient déjà été entreprises, ou soient envisagées, dans la plupart des États membres, elles diffèrent largement par leur calendrier, la nature des informations fournies, le public visé et les parties impliquées. Certains États membres ont toutefois préféré attendre jusqu'à la mise en place de la législation. Chaque fois qu'une consultation publique sur la mise en œuvre de la directive 2002/58/CE a été organisée, elle a contribué dans une certaine mesure à la sensibilisation.

Différentes autorités (par exemple les autorités chargées de la protection des données, les ARN, les autorités chargées de la protection des consommateurs, l'ombudsman) peuvent être responsables de ces activités, en fonction de leurs pouvoirs respectifs dans un État membre donné. Il n'existe pas (encore) de coordination entre les différentes autorités compétentes dans tous les États membres. Il semble que des ministères soient concernés dans certains États membres. La participation d'associations du secteur d'activité est fréquente. Parfois, des associations de consommateurs ou d'utilisateurs prennent également part à ces activités.

Certains acteurs de l'industrie ont également entrepris des activités de sensibilisation à l'échelle nationale, européenne ou mondiale, mais là aussi, les différences peuvent être considérables. Ces activités comprennent notamment:

- des guides pratiques destinés aux sociétés de vente directe, ou des campagnes spécifiquement conçues pour le secteur des communications;
- des conseils généraux à la clientèle sur les codes de conduite, les mécanismes de dépôt de plainte et le filtrage;

---

[39] Voir: http://www.dti.gov.uk/industries/ecommunications/directive_on_privacy_electronic_communications_200258ec.html#guidance

– des plateformes/groupes de travail chargés d'élaborer de bonnes pratiques pour les communications commerciales.

5.2. Actions proposées

Afin de parvenir à un niveau de connaissance élevé de ce qu'il faut faire (ou ne pas faire) en matière de message électronique commercial, une action de grande envergure et durable est nécessaire à court terme dans tous les États membres, tant sur le terrain de la prévention que sur celui de l'application des règles. Il convient de fournir des informations pratiques sur la prévention, les pratiques de prospection commerciale acceptables, ainsi que sur les solutions techniques et juridiques à la disposition des utilisateurs.

Toutes les parties sont invitées à jouer le rôle qui leur revient dans les activités de sensibilisation, depuis les États membres et les autorités compétentes jusqu'aux associations de consommateurs et d'utilisateurs, en passant par les entreprises. Les États membres et les autorités compétentes qui ne l'ont pas encore fait sont invités à lancer ou à soutenir des campagnes de sensibilisation au début de 2004.

Le programme Safer Internet et le spam

La Commission européenne a publié un appel de propositions dans le cadre du programme «Safer Internet», où des projets de lutte contre le spam pourraient être proposés au titre de différentes actions, par exemple en matière de sensibilisation. Les projets sélectionnés dans le cadre de la première évaluation de cet appel pourraient débuter en mai 2004.

La Commission prépare actuellement une proposition de programme de suivi, Safer Internet *plus*, qui proposera de financer d'autres mesures pour lutter contre les contenus illicites, préjudiciables et non souhaités tels que le spam.

http://www.europa.eu.int/information_society/programmes/iap/call/index_en.htm

En ce qui concerne en particulier la nature des informations fournies, les activités visant les entreprises et/ou les consommateurs devraient comprendre les éléments suivants:

– des explications de base, mais largement diffusées, sur les nouvelles règles et les droits dont jouissent les entreprises et/ou les consommateurs en vertu de celles-ci;

– des informations pratiques sur les pratiques de prospection commerciale acceptables dans le cadre du régime «opt-in», clarifiant notamment la notion de collecte légitime de données à caractère personnel;

– des informations pratiques sur la manière dont les consommateurs peuvent éviter le spam (par ex. utilisation des données à caractère personnel, etc.);

– des informations pratiques à l'intention des consommateurs concernant les produits et services disponibles pour éviter le spam (par exemple filtrage, sécurité);

– des informations sur les mesures pratiques à prendre en cas de réception de spam, y compris sur les mécanismes de dépôt de plainte et les formules substitutives de règlement des différends éventuellement disponibles.

Ces actions devraient toucher les groupes cibles suivants:
a) les entreprises pratiquant la vente directe ou y ayant recours,
b) les consommateurs qui s'abonnent à des services de courrier électronique, y compris les services SMS,
c) les fournisseurs de services de courrier électronique, y compris les fournisseurs de services mobiles.

Ces activités de sensibilisation devraient être menées par différents canaux (et pas uniquement au travers du web), en vue de toucher efficacement les différents publics visés. La participation de l'industrie et des associations de consommateurs est importante à cet égard. Il convient d'assurer la coordination des diverses initiatives éventuelles.

Les actions énumérées ci-dessus devraient aussi faire référence aux codes de conduite du secteur reconnus comme efficaces, aux mécanismes de dépôt de plainte, aux labels (par ex. labels de confiance) et aux systèmes de certification éventuellement disponibles.

Les services de la Commission fournissent déjà des informations sur les bases du régime «opt-in» sur le site web EUROPA[40]. Ils renverront également, grâce à des hyperliens, aux aspects nationaux de la mise en œuvre ainsi qu'aux statistiques de base disponibles et aux tendances en matière de spam. Les services de la Commission feront aussi appel aux Euro Info Centres afin de diffuser des informations sur les nouvelles règles.

CONCLUSION

Le spam est l'un des principaux défis auxquels l'internet est confronté actuellement. Il faudra, pour lutter contre ce phénomène, agir sur différents fronts: il s'agit non seulement d'être efficace dans l'application des règles et la coopération internationale, mais aussi d'amener l'industrie à adopter des solutions d'autorégulation et des solutions techniques, et de sensibiliser les consommateurs. Le tableau ci-dessous contient une synthèse des différentes actions répertoriées dans la présente communication.

La Commission soutiendra évidemment ces efforts dans la mesure du possible, mais il incombera surtout aux États membres de l'UE et à leurs autorités compétentes, à l'industrie et aux consommateurs et utilisateurs de l'internet et des services de communications électroniques de jouer leur rôle, aux niveaux national et international.

Une mise en œuvre intégrée et en parallèle de l'ensemble d'actions répertoriées dans la présente communication, qui bénéficie d'un large soutien de la part des parties concernées, peut contribuer à réduire considérablement le volume de spam qui compromet actuellement les avantages du courrier électronique et d'autres moyens de communication électronique pour nos sociétés et nos économies.

La Commission suivra de près la mise en œuvre de ces actions en 2004, notamment par l'intermédiaire du groupe informel sur les communications non sollicitées. Elle examinera, au plus tard pour la fin de 2004, si des actions supplémentaires ou des actions correctives sont nécessaires.

---

[40] Voir: http://europa.eu.int/information_society/topics/ecomm/highlights/current_spotlights/spam/index_en.htm

TABLEAU DES ACTIONS REPERTORIEES DANS LA COMMUNICATION

Le tableau ci-dessous récapitule les actions répertoriées dans la communication. Les actions relevant de la Commission et des services de la Commission ont été classées séparément. Comme indiqué ci-dessus, les actions sont liées entre elles de plusieurs manières et devraient être mises en œuvre autant que possible en parallèle et de manière intégrée.

I - Mise en œuvre et application effectives par les États membres et leurs autorités compétentes

Une condition préalable est la transposition, sans retard supplémentaire, de la directive «vie privée et communications électroniques» par les États membres, et notamment des dispositions relatives aux communications non sollicitées.

Les États membres et les autorités compétentes devraient évaluer l'efficacité de leurs mécanismes d'application (recours et sanctions, mécanismes de plainte, coopération interne à l'Union européenne et coopération avec les pays tiers, surveillance). Les États membres devraient également élaborer des stratégies nationales afin d'assurer la coopération entre les autorités chargées de la protection des données, les autorités chargées de la protection des consommateurs et les ARN, et éviter le chevauchement de compétences et la répétition inutile du travail entre les différentes autorités.

Les États membres et les autorités compétentes devraient notamment veiller aux aspects suivants:

a) Recours et sanctions efficaces

- offrir aux victimes des possibilités adéquates de réclamer des dommages-intérêts et prévoir de véritables sanctions, y compris financières, ainsi que des sanctions pénales le cas échéant;

- dans les États membres qui ne disposent pas de voie de recours administratif, envisager la création d'un tel recours afin de faire appliquer les nouvelles règles;

- doter les autorités compétentes des pouvoirs d'investigation et d'exécution nécessaires;

b) Mécanismes de plainte

- établir des mécanismes de dépôt de plainte appropriés, y compris des boîtes aux lettres électroniques qui recueilleront les plaintes des utilisateurs;

- coordonner l'action des différentes autorités nationales compétentes;

c) Plaintes transfrontalières et coopération en matière d'application à l'intérieur de l'UE

- utiliser un mécanisme de liaison existant (ou en créer un) pour permettre aux autorités nationales de coopérer afin de faire appliquer les règles à une échelle transfrontalière sur le territoire de l'UE (échange d'informations, assistance mutuelle). Dans ce cadre, en ce qui concerne en particulier le spam frauduleux et trompeur, le Conseil et le Parlement sont invités à se mettre d'accord aussi rapidement que possible sur la proposition de règlement relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs, et à étudier dans quelle mesure il faudrait ajouter la directive «vie privée et communications électroniques» au champ d'application dudit règlement;

d) Coopération avec les pays tiers

- participer activement aux forums multilatéraux (par exemple l'OCDE) afin d'élaborer des solutions au niveau international;

- renforcer la coopération bilatérale avec les pays tiers, ou engager une telle coopération;

- étudier, avec la Commission, quelle initiative spécifique elle pourrait prendre pour faciliter la coopération internationale;

- coopérer avec le secteur privé afin de dépister les «spammeurs», sous réserve des garanties juridiques appropriées.

(e) Monitoring

- veiller à disposer des informations et des statistiques requises pour cibler les efforts d'application, en coopération avec l'industrie le cas échéant, et en tenant compte du travail sur la mesure du spam en cours à l'OCDE.

II – Actions d'autorégulation et actions techniques de la part de l'industrie

Les acteurs du marché (par exemple les ISP, les ESP, les opérateurs de réseaux mobiles, les sociétés de développement de logiciels, les sociétés de marketing direct) devraient chercher à faire du régime «opt-in» une pratique quotidienne, en coopération avec les associations de consommateurs et d'utilisateurs et les autorités compétentes si nécessaire, et prévoir notamment les actions suivantes:

a) Actions d'autorégulation

- évaluer, et au besoin adapter, les pratiques contractuelles des fournisseurs de services (ISP, ESP, opérateurs mobiles) envers leurs abonnés et partenaires commerciaux; fournir des informations sur le filtrage et éventuellement fournir un logiciel ou un service de filtrage à titre de service clientèle optionnel;

- adapter les pratiques de prospection directe au régime «opt-in» et éventuellement se mettre d'accord sur des méthodes spécifiques et conformes au droit pour collecter des données à caractère personnel (par ex. système à 'inclusion confirmée ou « confirmed opt-in »);

- élaborer et diffuser des codes de bonnes pratiques efficaces (par exemple l'initiative FEDMA) conformes au régime «opt-in», en coopération avec le groupe de travail «article 29» sur la protection des données ou avec les autorités nationales compétentes le cas échéant;

- envisager l'utilisation de labels pour les messages électroniques et les bases de données qui respectent le régime «opt-in» pour aider les utilisateurs (et les filtres) à les reconnaître, en conformité avec la directive sur le commerce électronique;

- utiliser, ou créer si nécessaire, dans le cadre de l'autorégulation, des mécanismes de plainte et des systèmes alternatifs de règlement des conflits qui soient efficaces et reposent sur des initiatives existantes dans la mesure du possible (par ex. EEJ-NET).

b) Actions techniques

- (Les fournisseurs de logiciels de filtrage doivent) veiller à ce que leurs systèmes de filtrage soient compatibles avec le régime «opt-in» et d'autres exigences du droit de l'UE, y compris celles liées à la confidentialité des communications. Les États membres et les autorités compétentes sont invités à clarifier les conditions juridiques dans lesquelles différents types de logiciels de filtrage peuvent fonctionner dans le pays concerné, y compris sous l'angle du respect de la vie privée.

- (Les fournisseurs de logiciels de filtrage doivent) tenir compte des conséquences, pour les utilisateurs, des cas de «faux positif», de «faux négatif», de certaines formes de filtrage fondé sur le contenu, et des problèmes de responsabilité qui risquent d'y être associées. Les utilisateurs devraient avoir la possibilité de déterminer la manière dont le spam entrant est géré, en fonction de leurs besoins.

- (Les fournisseurs de logiciels de filtrage devraient) coopérer avec les parties concernées pour développer des techniques de reconnaissance des courriels commerciaux légitimes (c'est-à-dire correspondant aux pratiques commerciales acceptées en vertu du droit communautaire), en utilisant par exemple des labels.

- (Les fournisseurs de services de courrier électronique, et de services mobiles le cas échéant devraient) offrir en option des équipements ou des services de filtrage aux clients qui en font la demande, et les informer sur ceux proposés par des tiers.

- (Les propriétaires de serveurs de courrier électronique devraient) s'assurer que leurs serveurs sont correctement sécurisés et ne se trouvent pas en mode «open relay» (si cela n'est pas justifié). La même remarque vaut pour les serveurs proxy ouverts.

III - Actions de sensibilisation à mener par les États membres, le secteur d'activité et les associations de consommateurs/d'utilisateurs

Les États membres et les autorités compétentes qui ne l'ont pas encore fait sont invités à lancer ou à soutenir des campagnes de sensibilisation au début de 2004.

Toutes les parties concernées, depuis les États membres et les autorités compétentes jusqu'aux associations de consommateurs et/ou d'utilisateurs, en passant par les entreprises et le secteur d'activité, devraient jouer un rôle actif dans des campagnes d'information pratique sur la prévention, les pratiques de prospection commerciale acceptables, et sur les solutions techniques et juridiques qui s'offrent aux utilisateurs, et devraient notamment:

- cibler leurs actions sur: a) les entreprises pratiquant la vente directe ou y ayant recours, b) les consommateurs qui s'abonnent à des services de courrier électronique, y compris les services SMS et c) les fournisseurs de services de courrier électronique, y compris les fournisseurs de services mobiles;

fournir aux entreprises et/ou aux consommateurs:

– des explications de base, mais largement diffusées, sur les nouvelles règles et les droits dont ils jouissent en vertu de celles-ci;

– des informations pratiques sur les pratiques de prospection commerciale acceptables dans le cadre du régime «opt-in», clarifiant notamment la notion de collecte légitime de données à caractère personnel;

– des informations pratiques sur la manière dont les consommateurs peuvent éviter le spam (par ex. utilisation des données à caractère personnel, etc.);

– des informations pratiques à l'intention des consommateurs concernant les produits et services disponibles pour éviter le spam (par exemple filtrage, sécurité);

– des informations sur les mesures pratiques à prendre en cas de réception de spam, y compris sur les mécanismes de plainte et les systèmes alternatifs de règlement des conflits éventuellement disponibles;

- faire référence aux codes de conduite du secteur reconnus comme efficaces, aux mécanismes de plainte, aux labels (par ex. labels de confiance) et aux systèmes de certification éventuellement disponibles;

- déployer ces activités de sensibilisation en empruntant différents canaux, en ligne et hors ligne, en vue de toucher efficacement les différents publics visés.

La participation du secteur d'activité et des associations de consommateurs est importante à cet égard. Il convient d'assurer la coordination des diverses initiatives possibles.

IV – Actions à mettre en œuvre par la Commission et ses services

La Commission surveillera la mise en œuvre des actions résumées ci-dessus au cours de l'année 2004, notamment par l'intermédiaire du groupe informel sur les communications non sollicitées, et elle évaluera au plus tard fin 2004 si des actions supplémentaires ou des actions correctives sont nécessaires.

La Commission continuera à surveiller attentivement la mise en œuvre de la directive. Elle s'attachera notamment à vérifier que les mesures de transposition nationales prévoient bien de véritables sanctions, y compris financières ou pénales, en cas de violation des exigences de la directive. (La Commission a lancé en novembre 2003 des procédures d'infraction à l'encontre de plusieurs États membres qui ne lui ont pas notifié leurs mesures de transposition nationales.) Les services de la Commission sont disposés à aider les États membres si cela s'avère nécessaire.

Les services de la Commission ont créé un «groupe en ligne informel sur les communications commerciales non sollicitées», avec l'appui des États membres et des autorités chargées de la protection des données. Ce groupe facilitera le travail sur l'application effective de la directive (par ex. en matière de plaintes, de recours, de sanctions, de coopération internationale) ainsi que sur les autres actions répertoriées dans la présente communication.

Les services de la Commission demanderont au groupe de travail «article 29» sur la protection des données d'adopter dans les meilleurs délais un avis sur certaines notions utilisées dans la directive «vie privée et communications électroniques», afin de contribuer à une application uniforme des mesures nationales prises en vertu de la directive.

Les services de la Commission ont commencé à étudier, avec les États membres et les autorités nationales chargées de l'application de la directive, les meilleurs moyens d'assurer son application transfrontalière sur le territoire de l'UE, ainsi qu'avec les pays tiers. Ce travail mené avec les autorités nationales se poursuivra tout au long de l'année 2004.

La Commission soutiendra le lancement, à l'échelle paneuropéenne, de codes de conduite en ligne pour la vente directe, et le cas échéant leur approbation par le groupe de travail «article 29» sur la protection des données.

La Commission accueillera un atelier de l'OCDE sur le spam en février 2004 et examinera avec les États membres les actions de suivi à mener, y compris les efforts de l'OCDE pour promouvoir une législation efficace à l'échelon international, la sensibilisation, les solutions techniques, l'autorégulation et la coopération internationale sur l'application des règles.

La Commission s'efforcera de déterminer les meilleurs moyens d'assurer le suivi des résultats du sommet mondial de 2003 sur la société de l'information dans l'UE en prévision de la phase de Tunis qui aura lieu en 2005.

La Commission a publié un appel à propositions dans le cadre du programme «Safer Internet», où des projets de lutte contre le spam pourraient être proposés au titre de différentes actions; la Commission prépare actuellement une proposition de programme de suivi, Safer Internet *plus*, qui proposera de financer des mesures supplémentaires notamment pour lutter contre le spam.

Les services de la Commission continueront à fournir, sur le site web EUROPA, des informations sur les bases du régime «opt-in». Au moyen d'hyperliens, elle renverra également aux aspects nationaux de la mise en œuvre ainsi qu'aux statistiques de base disponibles et aux tendances en matière de spam. Les services de la Commission feront aussi appel aux Euro Info Centres afin de diffuser des informations sur les nouvelles règles.