Directive pour le marketing en ligne acceptable de l'association «eco – Verband der Internetwirtschaft e.V.»

Lignes directrices pour la pratique

6e édition 2016

ACTUALISÉE
Liste globale d´opt-in et d´opt-out

éditée par

CSA
Certified Senders Alliance

eco
ASSOCIATION OF THE INTERNET INDUSTRY
WE ARE SHAPING THE INTERNET.
YESTERDAY. TODAY. BEYOND TOMORROW.

CONTENU

1. Préambule

En 2002, le groupe de compétence pour le marketing en ligne de l'association « eco-Verband der Internetwirtschaft e. V. » a adopté la première « directive pour le marketing en ligne souhaité ». Depuis, la directive a été régulièrement mise à jour et plus d'un million d'exemplaires du guide recherché a été distribué ou téléchargé au format pdf du site web eco.

Cette nouvelle version de la directive tient compte de toute une série de jugements plus récents (p. ex. le jugement prononcé par la cour fédérale de justice BGH, Bundesgerichtshof) portant sur les réponses automatiques aux courriels). Il y a lieu de rappeler les conséquences résultant du nouveau règlement général relatif à la protection des données qui sera applicable à compter du 25 mai 2018. Ce règlement entre immédiatement et directement en vigueur, sans qu'il ne soit nécessaire de le faire passer en droit national. Les mesures publicitaires contraires à la loi et les violations de la protection des données pourront alors être sanctionnées d'amendes nettement plus élevées, allant jusqu'à 20 millions d'euros.

La vaste liste des pays pour lesquels les bases juridiques du marketing par courriel ont été expliquées a été complétée. Les chapitres ont été élargis à la situation juridique en Autriche et de la Suisse.

Le marketing par courriel continue à constituer une partie intégrale et essentielle de la communication de beaucoup d'entreprises avec leurs clients. Afin d'expliciter les particularités quant à la conformité juridique de cette communication de marketing, le présent guide fournit des instructions concrètes et notamment proches de la réalité. La présente directive répond aux questions juridiques les plus fréquentes que se posent les entreprises. Chacune des questions comporte trois domaines :

1. les prescriptions réglementaires ;
2. une explication de la question et des propositions pour la mise en œuvre des prescriptions réglementaires ;
3. des exemples pratiques.

Les questions juridiques prioritaires du point de vue de l'entreprise lors de l'envoi de courriels sont :

- Est-ce que l'on dispose du consentement des destinataires ?
- Est-ce qu'il est possible de prouver ce consentement ?
- Est-ce que les destinataires savent à quoi ils ont consenti ?
- Est-ce que les destinataires ont été informés de leur faculté de révoquer leur consentement qui, en plus, ne doit occasionner ni frais ni difficultés ?
- Est-ce que les destinataires reçoivent une confirmation par courriel de leur consentement ?
- Est-ce que l'on répond aux demandes ?
- Est-ce que l'objet ne risque pas d'induire à l'erreur ?
- Est-ce que l'expéditeur est facilement identifiable ?
- Est-ce que les mentions légales sont complètes ?
- S'agit-il ici d'un cas de traitement de données par des prestataires de services tiers et est-ce que les prescriptions légales y afférentes ont été respectées ?

Bien entendu, la présente directive ne saurait remplacer une consultation juridique dans

des cas bien spécifiques. Elle pourra toutefois contribuer à ce que les entreprises obtiennent davantage d'assurance en se servant du médium du courriel voire du marketing direct lors des contacts avec des prospects. De même, les consommateurs doivent se sentir plus en sécurité lorsqu'ils laissent leur adresse courriel à une entreprise. « En sécurité » signifie dans ce contexte que les adresses ne sont pas tout simplement remises à des tiers, que les courriels ne sont envoyés qu'avec le consentement du destinataire et qu'il est possible sans aucun problème de supprimer sa propre adresse de la liste de distribution à tout moment.

Le grand succès du médium qu'est le courriel est basé sur la confiance. La présente directive veut y contribuer. La directive peut également être consultée via internet sous **https://certified-senders.eu/documents**.

2. Permission

De nos jours, nul n'est censé ignorer que la publicité via courriel requiert toujours le consentement du destinataire, que ce soit dans le domaine B2C ou celui du B2B. On peut résumer succinctement les conditions préalables pour un consentement valable comme suit :

- transparent ;
- volontaire ;
- conscient, indubitable, clair et
- séparé.

Par ailleurs, il doit être possible de prouver le consentement qui doit faire l'objet d'un procès-verbal détaillé. Pour la publication par courriel dans le cadre de relations clients déjà nouées, la loi prévoit certains allègements (cf. chapitre 2.12).

2.1 Bases juridiques

Au niveau européen, c'est la directive relative à la vie privée et aux communications électroniques (également connue en tant que directive ePrivacy) qui stipule à l'article 13 déjà que l'envoi de publicité par courriel requiert le consentement du destinataire. De ce fait, cette stipulation de base vaut de la même manière pour tous les états membres de l'UE. Or, les directives de l´UE ne sont pas applicables directement mais doivent être transposées, dans chacun des états membres, en droit national. C'est au moment de cette transposition en droit national que surviennent des différences juridiques qui sont souvent non négligeables. En plus, les tribunaux nationaux et les autorités chargées de la protection des données font souvent une interprétation différente aux lois. Par conséquent, le droit relatif au marketing par courriel repose, certes, sur une base européenne homogène, mais dans les détails, on peut toutefois constater certaines différences (cf. à ce sujet également l'exposé sommaire sur la situation juridique dans les différents pays au chapitre 10).

En Allemagne, les prescriptions de l'Union Européenne sur la publicité par courriel ont été transposées en droit national avec la loi fédérale sur la protection des données (Bundesdatenschutzgesetz, BDSG), la loi sur les télémédias (Telemediengesetz, TMG) et la loi sur la concurrence déloyale (Gesetz gegen den unlauteren Wettbewerb, UWG). La nécessité du consentement à la publicité par courriel résulte des article 7, paragraphe 2 de la loi UWG et de l'article 28, paragraphe 3, phrase 1 de la loi BDSG.

Aussi simple que puisse paraître le principe « publicité par courriel uniquement en cas de consentement », aussi complexe est pourtant sa mise en œuvre dans le détail. Par ailleurs, de nombreux jugements et modifications des lois ne cessent de modifier les prescriptions relatives aux déclarations de consentement juridiquement valables (en règle générale, en les renforçant).

Une modification de la législation à venir se fait déjà sentir à l'heure actuelle : le règlement général de la CE relatif à la protection des données.

Le nouveau règlement général de l'UE relatif à la protection des données qui sera applicable à compter du 25 mai 2018, sera en vigueur immédiatement et directement sans qu'il ne soit nécessaire de le faire passer en droit national. Il vise parmi d'autres une harmonisation du droit de la protection des données au sein de l'UE. En ce qui concerne l'Allemagne, la situation juridique dans son ensemble concernant le consentement et la licéité de la publicité par courriel sera maintenue. Les mesures publicitaires contraires à la loi, toutefois, pourront être sanctionnées par des amendes nettement plus importantes, la sanction maximale prévue pour les violations de la protection des données passe à une amende de 20 millions euros ou 4% du chiffre d'affaire annuel réalisé dans le monde entier par une entreprise (le chiffre le plus élevé faisant foi).

2.2 Définition du terme publicité

Le consentement du destinataire est nécessaire lorsque le courriel représente de la publicité. Se pose alors la question de savoir ce qui est à qualifier de publicité du point de vue juridique.

Pour ce qui concerne la question de savoir ce qui est à considérer comme publicité, la législation et la juridiction n'y vont pas de main morte. Tout propos servant de loin ou de près, directement ou indirectement, à vendre des produits et des services, tombe sous la définition de « publicité ». Comme le dit si bien le juriste, il y a lieu d'interpréter le terme de la publicité « de manière large ». Ainsi, la législation considère comme publicité par exemple même les vœux d'anniversaire ou de Noël envoyés par une entreprise à ses clients par courriel ainsi que les courriels servant à une étude du marché qui n'est pas réalisée de manière neutre mais dans l'intérêt de l'entreprise. Presque tout ce que fait une entreprise et toute sa communication vers l'extérieur sert, en fin de compte, à vendre des produits et des services. Ceci englobe p. ex. aussi la publicité dite publicité favorisant la demande ou de pures relations publiques (publicité pour une marque sans aucun lien avec un produit spécifique), tout comme les nouvelles dites de service comportant des renseignements sur d'autres produits, étant donné que ces renseignements aussi servent indirectement à stimuler les ventes.

Même la publicité faite par les partis politiques lors des élections ainsi que la publicité pour collecter des dons par les organisations charitables tombent sous la définition de la publicité.

2.3 Consentement transparent

Pour être valable, un consentement doit répondre à certains critères de forme et de

contenu. Le point essentiel, c'est tout d'abord que la personne consentante soit informée de manière transparente et compréhensible du contenu de son consentement. Selon l'article 4bis, paragraphe 1, phrase 2 de la loi BDSG et de la jurisprudence en résultant, prononcée par la cour fédérale de justice BGH le 25 octobre 2012, réf. I R 169/10, un consentement n'est valable que s'il est donné en toute connaissance de cause et s'il est expliqué pour le cas concret. La personne consentante doit être en mesure de se faire une idée concrète des personnes exploitant ses données, ainsi que dans quel but ceci est fait.

L'entreprise voulant plus tard se réclamer du consentement doit clairement être indiquée. Le consentement ne vaut alors toujours que pour l'entreprise expressément spécifiée. Il n'existe aucun « consentement en blanc » susceptible de permettre à une entreprise XY et les « entreprises partenaires » de celle-ci de procéder à la publicité par courriel. Le droit de la protection des données ne connaît pas non plus de privilège accordé aux groupes. Même une transmission d'adresses de courriel au sein d'un groupe dans le but d'une exploitation à des fins publicitaires par d'autres entreprises du groupe est illicite (sauf si les entreprises du groupe sont expressément citées dans le consentement). Il est à supposer qu'une indication globale d'une entreprise XY « et ses entreprises liées » constituerait également une violation de l'impératif de transparence.

Il conviendrait que la déclaration de consentement explique également le contenu des courriels de publicité à envoyer de manière aussi transparente que possible. Lorsque, par exemple, une entreprise distribue différentes lignes de produits sous des marques différentes, la déclaration de consentement doit spécifier si le destinataire recevra désormais exclusivement de la publicité pour la ligne de produits sous la marque X ou si ce seront toutes les marques de l'entreprise pour lesquelles il y aura de la publicité.

Worst Practice/exemples négatifs :

☐ Je consens à l'exploitation de mes données à des fins publicitaires. Je peux révoquer mon consentement à tout moment par courriel adressé à unsubscribe@abd.de.

Une telle déclaration de consentement est nulle et non avenue étant donné qu'elle ne spécifie pas les médias (courriel, texto, téléphone, courrier) qui seront utilisés pour la publicité.

☐ Je souhaite recevoir de la publicité par courriel par la société ABC GmbH et les entreprises partenaires de la société ABC GmbH. Je peux révoquer mon consentement à tout moment par courriel adressé à unsubscribe@abc.de. Par ailleurs, chaque courriel comportera un lien permettant d'annuler l'envoi d'informations supplémentaires.

Cette déclaration de consentement ne spécifie pas au destinataire de quelles entreprises partenaires il s'agit. De ce fait, la personne consentante n'a aucune idée à quelles entreprises son adresse courriel est transmise. Un consentement englobant également la transmission à des tiers doit spécifier dans les détails les destinataires potentiels des données.

2.4 Déclaration consciente, indubitable et explicite

De plus, le consentement doit être donné par la personne consentante en conformité avec l'article 7, paragraphe 2, point 3 de la loi UWG, de manière expresse, c'est-à-dire consciemment et activement. Ceci peut se faire par écrit, à travers une signature de la personne consentante ou par voie électronique en cliquant sur une case à cocher. De ce fait, une possibilité de refus, par exemple une case à cocher sur laquelle on peut cliquer si l'on ne souhaite pas recevoir de publicité par courriel ou bien une case à cocher déjà cochée ne constitue pas de déclaration de consentement valable. La publication d'une adresse courriel dans des registres publics, sur des pages internet, dans un en-tête de lettre ou sur une carte de visite n'est pas non plus un consentement pour la réception de publicité par courriel. Un consentement présumé voire implicite laissant seulement supposer un intérêt de la part du destinataire ne suffit plus.

Le consentement à la réception d'une publicité par courriel doit toujours être donné de manière séparée, c'est-à-dire qu'il ne saurait être combiné avec d'autres déclarations. Par conséquent, il y a lieu de prévoir deux cases à cocher séparément pour la confirmation d'un achat dans une boutique en ligne (« Valider la commande et déclencher l'obligation de paiement ») d'une part et le consentement à la publication par courriel d'autre part. C'est ce qui a été re-confirmé par la cour fédérale de justice BGH dans son jugement dit « jugement Payback » (jugement du 16 juillet 2008, réf. VIII ZR 348/06).

Le libellé de la déclaration du consentement doit, lui aussi, spécifier indubitablement qu'il s'agit d'un consentement qui est en train d'être donné. Par exemple, la phrase « Je sais que… » ne suffit pas, étant donné que la personne consentante n'est alors pas forcément consciente du fait qu'elle est en train de fournir une déclaration de consentement. C'est sur ce fait que le « Düsseldorfer Kreis » (« cercle de Düsseldorf ») attire l'attention dans son « Orientierungshilfe zur datenschutzrechtlichen Einwilligungserklärung in Formularen » utile datant du mois de mars 2016.

Worst Practice/exemple négatif :

☐ Je ne voudrais PAS recevoir de courriel comportant la newsletter de la société ABC GmbH.

Le refus déclaré ici ne représente pas une déclaration de consentement valable. Le consentement doit être donné par un acte réalisé activement par la personne consentante. Or, dans l'exemple qui nous préoccupe, la personne consentante doit agir quand elle ne veut justement pas donner son consentement.

Best Practice/exemple positif :

☐ Je souhaite recevoir par courriel la newsletter hebdomadaire de la société ABC GmbH comportant des informations relatives à ses offres du domaine des télécommunications. En aucun cas, mes données ne seront transmises à des tiers. Je peux révoquer mon consentement à tout moment par courriel adressé à unsubscribe@abc.de avec effet pour

l'avenir. Par ailleurs, chaque courriel comportera un lien permettant d'annuler l'envoi d'informations supplémentaires.

Cette déclaration de consentement répond aux prescriptions légales.

2.5 Exigences quant à la forme du consentement

Consentement donné par carte postale ou par lettre : un consentement doit toujours être donné par écrit (article 4bis, paragraphe 1, phrase 3 de la loi BDSG). Par « forme écrite », la loi entend la signature manuscrite de la personne consentante. Donc, si le consentement est donné par exemple dans un document - comme une carte postale ou une lettre - qui a été signé par le destinataire ultérieur du courriel publicitaire, il est possible de prouver le consentement moyennant ce document. À cet effet, il y a lieu de conserver ce document impérativement.

Consentement en ligne : l'internet permet également de donner un consentement électronique. Conformément aux dispositions de l'article 13, paragraphe 2 de la loi TMG, un consentement électronique doit répondre à certaines exigences de forme, à savoir:

- le consentement doit faire l'objet d'un procès-verbal ;
- l'utilisateur doit être en mesure d'appeler le contenu de son consentement à tout moment ; et
- l'utilisateur doit être en mesure de révoquer son consentement à tout moment avec effet pour l'avenir. Il y a lieu d'attirer au préalable l'attention sur ce droit de révocation (article 13, paragraphe 3 de la loi TMG).

Consentement donné lors d'un contact personnel et au téléphone : un consentement peut également être donné par téléphone ou personnellement, par exemple dans le cadre d'un appel dans un centre d'appels ou « face à face » sur un salon. Depuis la réforme du droit de la protection des données en 2009, ce type de consentement qui n'a pas été donné par écrit ou par voie électronique au sens de l'article 13 de la loi TMG, doit toutefois être confirmé par écrit (article 28, paragraphe 3, lettre a) de la loi BDSG).

2.6 Minimisation des données

Dans le cadre du consentement, il est prohibé de demander au destinataire plus de données qu'effectivement nécessaires pour la prestation des services. En règle générale, il suffit, pour envoyer une newsletter par courriel, de demander la seule adresse courriel. Toutes les autorités chargées de la protection des données ne considèrent pas comme licite une demande de divulgation obligatoire du prénom ou du nom de famille afin de personnaliser le courriel comportant la newsletter. Il est toutefois possible de demander un nombre illimité de données à titre volontaire.

2.7 Co-enregistrement et achat d'adresses

Au moment de la collecte des coordonnées pour des tiers (génération de leads à travers un co-enregistrement), aussi, il y a lieu de désigner dans les détails les entreprises pour lesquelles les adresses doivent être collectées. Le nombre d'entreprises pour lesquelles des adresses doivent être collectées parallèlement, doit alors rester limité. Il est recommandable de respecter

notamment les conditions préalables suivantes :

- il y a lieu de spécifier individuellement les noms des entreprises pour lesquelles des coordonnées sont générées, ainsi que les branches auxquelles elles appartiennent ;
- il doit être facile et clair pour l'utilisateur de prendre connaissance de la liste des entreprises au cours du processus de son consentement ;
- la liste est limitée à un maximum de 10 (dix) entreprises.

Il y a lieu de supposer que la limite de la clarté est dans tous les cas dépassée lorsque l'utilisateur ne saurait plus distinguer les entreprises concernées « d'un coup d'œil ».

L'utilisation d'adresses courriel achetées est sujette à des obligations de vérification plus strictes. En effet et conformément à la jurisprudence, l'acheteur des adresses courriel doit s'assurer que le titulaire des différentes adresses courriel soit effectivement d'accord avec la réception de la publicité et que les consentements donnés valablement ne concernent notamment pas seulement l'envoi par le vendeur mais également par des tiers (en l'occurrence, par l'acheteur). Il ne suffit alors pas de se fier à l'assurance donnée par le vendeur affirmant que les consentements ont été fournis. L'acheteur est tenu de se faire produire les justificatifs documentés correspondants et de procéder au moins à une vérification par échantillons. Donc, afin d'être absolument sûr dans ce domaine, il conviendrait de ne pas se contenter d'une simple production des justificatifs des consentements mais de les conserver dans ses propres dossiers à des fins de documentation.

2.8 Consentement fourni par des mineurs

L'âge minimum permettant de donner un consentement n'est pas défini avec précision. Dans le cadre d'une publicité par courriel, on peut en principe considérer qu'un mineur est capable de donner son consentement à partir de l'âge de 16 ans. Mais en ce qui concerne le consentement au traitement de données dites « sensibles » (p. ex. la santé, l'appartenance à une religion, etc.), il convient toutefois éventuellement d'appliquer des exigences plus strictes dans chaque cas individuel.

Pour la première fois, c'est le règlement général de la CE (qui s´applique à compter du 25 mai 2018) qui introduit au moins un début de clarté en fixant l'âge minimum permettant de donner un consentement à 16 ans, tout en garantissant aux états membres de la CE la faculté de prévoir une limite d'âge inférieure (minimum de 13 ans).

2.9 Durée de validité du consentement

Les affirmations selon lesquelles un consentement à la réception de publicité par courriel n'est plus en vigueur après un certain temps persistent avec ténacité. Or, même dans la jurisprudence, on ne trouve aucun indice laissant supposer l'existence d'une telle « durée de vie ».

Mais il convient de veiller à ce qu'un tel consentement soit exploité dans les meilleurs délais après sa fourniture. Selon l'avis du tribunal de grande instance de Munich I, exprimé dans son jugement du 8 avril 2010, réf. 17 HK O 138/10, un consentement à la réception de publicité par courriel et dont le

bénéficiaire aurait fait usage plus d'un an et demi plus tard seulement ne serait plus en vigueur, étant donné que la personne consentante ne s'attendrait plus à la réception de publicité après une période aussi longue. Mais lorsqu'un consentement est utilisé à des intervalles réguliers pour l'envoi de newsletters par courriel, il n'y a nullement lieu de présumer que ledit consentement puisse perdre sa validité après un certain temps.

2.10 Démontrabilité du consentement (double-opt-in)

Dans le cas d'un litige devant les tribunaux concernant la licéité de l'envoi de courriels de publicité, la charge de la preuve et de l'allégation de la fourniture effective du consentement donné par le titulaire en question de l'adresse courriel utilisé incombe à l'expéditeur. La seule déclaration selon laquelle un consentement à la réception de courriels de publicité à une adresse courriel spécifique a été donné ne saurait suffire lorsque l'expéditeur n'est pas en mesure de prouver que le consentement provient effectivement du titulaire de l'adresse courriel utilisé.

L'expéditeur est toujours tenu à se conformer à ce qui suit :

- la seule fourniture du consentement donné par le destinataire ne suffit pas. Le consentement doit être obtenu de sorte qu'il est possible d'en apporter la preuve à la satisfaction d'un tribunal (caractère démontrable) ;
- le seul consentement donné par une personne quelconque ne suffit pas non plus. Il y a lieu de démontrer que c'est précisément le destinataire qui a fourni le consentement, à l'exclusion d'un tiers potentiel ayant utilisé le nom ou l'adresse courriel de ce dernier (cohérence : inscripteur – (futur) destinataire).

C'est la procédure double-opt-in qui offre la plus grande sécurité juridique en tant que preuve justifiant que le consentement provient effectivement du titulaire de l'adresse courriel utilisée. Par conséquent, il convient de recommander l'utilisation de la procédure double-opt-in - sans qu'elle ne constitue pour autant une obligation légale. Même si on le lit à de maintes reprises : il n'existe aucune obligation légale d'utiliser la procédure double-opt-in. Une telle obligation n'a pas non plus été introduite par la nouvelle loi BDSG 2009.

Pourquoi en fait un double-opt-in ?

Pour mémoire et pour être clair : la procédure double-opt-in consiste à envoyer un courriel de confirmation (souvent aussi appelé courriel d'invitation ou courriel de contrôle) à une adresse courriel indiquée lors de l'inscription pour une newsletter. Dans ce courriel de confirmation, le destinataire est invité à confirmer son consentement en cliquant sur un lien de confirmation. Lorsque le destinataire clique sur le lien de confirmation, ceci permet d'apporter la preuve de ce que c'est effectivement le titulaire de l'adresse courriel indiqué au moment de l'inscription qui a donné le consentement.

L'utilisation de la procédure double-opt-in permet ainsi d'éviter des envois de courriels de publicité à une adresse courriel qui n'a pas été enregistrée par son titulaire mais de manière abusive par un tiers. De plus, cette

procédure garantit à ce qu'aucun courriel de publicité ne soit intégré dans la liste de distribution alors que l'utilisateur a juste commis une faute de frappe au moment de son inscription. Dans un tel cas de figure, il y a également des risques à ce que le titulaire effectif de l'adresse courriel reçoive des courriels de publicité alors qu'il n'y a jamais donné son consentement.

Et est-ce que la procédure double-opt-in est juridiquement infaillible ?

En principe, on trouve, dans le domaine du télémarketing, des jugements contradictoires sur pratiquement toutes les questions juridiques. Ainsi, les tribunaux ne furent et ne sont malheureusement toujours pas complètement d'accord entre eux sur l'appréciation de la procédure double-opt-in. Dans certains jugements, le seul courriel de confirmation a déjà été considéré comme une nuisance déraisonnable (voire de la publicité par courriel illicite, voire même du pourriel). Malheureusement, les tribunaux ont alors oublié le fait qu'il n'existe en fin de compte aucune alternative à la procédure double-opt-in si l'on souhaite procéder à du marketing par courriel tout en s'assurant de la sécurité juridique. En effet, ce n'est même pas lors d'une utilisation (certes, hypothétique) d'une procédure post-ident ou d'une authentification notariée du consentement à la réception de publicité par courriel qu'il est possible de déterminer de manière juridiquement sûre que, par exemple, l'adresse courriel ange23@gmx.de appartient réellement à Madame Dupont qui a justement indiqué cette adresse lors de la fourniture de son consentement.

Par conséquent, le fait que la cour fédérale de justice BGH, dans son jugement du 10 février 2011, réf. I ZR 164/09 portant - détail intéressant - le titre « procédure double-opt-in » ait donné son feu vert de principe à la procédure double-opt-in était un progrès non négligeable :

« En cas de réception d'une demande d'inscription par la voie électronique, il est possible de demander à l'expéditeur de confirmer sa demande d'inscription en lui envoyant un courriel. Après réception de la confirmation demandée, il est permis de présumer que la demande provient effectivement de l'adresse courriel indiquée. »

La cour d'appel de Munich a toutefois jugé le 27 septembre 2012 que déjà le courriel de confirmation dans le cadre de la procédure double-opt-in serait un courriel de publicité non sollicité. Le courriel de confirmation qui sert justement à éviter les pourriels serait alors, selon l'avis des juges Munichois, du pourriel, lui aussi.

Selon le jugement de Munich, cela signifierait la nécessité d'un consentement déjà pour ce courriel de confirmation. Mais étant donné que le courriel de confirmation sert justement à fournir la preuve du consentement, il ne serait par conséquent pas possible de se procurer un consentement démontrable pour l'envoi du courriel de confirmation. Alors, on se sent un petit peu comme dans un roman de Kafka :

« Vous souhaitez obtenir un consentement ? Alors, dans ce cas, veuillez tout d'abord prouver que vous disposez déjà d'un consentement… »

Ceci engendrait des problèmes simplement

impossibles à résoudre dans la pratique. L'envoi d'un courriel de confirmation dans le cadre d'une procédure double-opt-in est considéré comme licite dans les conditions préalables suivantes :

a) Courriel de confirmation sans publicité

Le courriel de confirmation doit toujours être absolument exempt de toute publicité et doit servir au seul but de vérifier l'adresse courriel.

Contrairement à ce qui est souvent avancé, il n'est pas nécessaire que le courriel de confirmation soit envoyé sous forme de texte clair. Il peut tout à fait répondre à l'identité graphique de l'entreprise et comporter par exemple un logo, mais il y a lieu d'éviter à tout prix tout élément de publicité supplémentaire. Un courriel de confirmation surchargé de publicité serait écarté par les tribunaux en tant que courriel de publicité illicite.

b) Courriel de confirmation comportant une déclaration de consentement complète

Le courriel de confirmation sert à la seule vérification du consentement. Si un utilisateur, lors d'une inscription pour une newsletter, indique l'adresse courriel d'un tiers de manière abusive ou encore parce qu'il estime que la newsletter pourrait intéresser le titulaire de l'adresse courriel, le titulaire de cette adresse courriel reçoit un courriel de confirmation. Il reçoit ce courriel sans avoir eu connaissance de la déclaration faite par le tiers et sans avoir jamais fourni une déclaration quelconque sur un site web. Si maintenant il clique sur le lien de confirmation, c'est ce seul clic qui doit constituer un consentement suffisant afin de lui envoyer à l'avenir la newsletter à son adresse courriel.

Par conséquent, le courriel de confirmation doit comporter le consentement intégral et le clic sur le lien de confirmation doit constituer un consentement à part entière. Le seul libellé du courriel de confirmation doit permettre à l'expéditeur de démontrer devant les tribunaux qu'il était en possession d'un consentement du destinataire des envois de courriels de publicité. Par conséquent, il ne suffit pas que le courriel de confirmation demande brièvement et succinctement de confirmer le consentement donné lors de l'inscription faite sur le site web sans pour autant reprendre ledit consentement.

En d'autres termes : si vous investissez beaucoup de temps et de travail (et éventuellement même de l'argent pour une appréciation juridique) dans le libellé de votre déclaration de consentement devant figurer sur votre site web, cette déclaration de consentement doit également être reprise fidèlement dans le courriel de confirmation. Dans le cas contraire, mieux vaut s'abstenir.

c) Courriel de confirmation sans autres déclarations

En plus, il convient que le courriel de confirmation serve uniquement à la confirmation du consentement, à l'exclusion de toutes déclarations complémentaires. L'une des conditions préalables formelles dont il y a désormais une multitude quant à la validité d'un consentement, c'est qu'elle doit être donnée séparément, donc en

principe de manière isolée des autres (cf. chapitre 2.2).

De ce fait, la confirmation du consentement contenu dans le courriel de confirmation ne doit pas être combinée avec la participation à une loterie, par exemple.

Worst Practice/exemple négatif

Un seul clic vous sépare du grand gain ! Veuillez finaliser votre participation à notre grande loterie permettant de gagner des millions et cliquez sur le lien suivant pour confirmer les conditions de participation à la loterie et votre abonnement de notre newsletter comportant des informations actuelles.

Ce cas de figure ne constitue plus de déclaration de consentement séparée et le consentement serait nul et non avenu. Le libellé de la confirmation à fournir doit clairement préciser que seul le consentement à la réception de la newsletter est confirmé, à l'exclusion de la participation concomitante à la loterie.

Best practice/exemple positif

Nous vous remercions de votre participation à notre grande loterie vous permettant de gagner des millions ! Merci de nous confirmer votre abonnement de notre newsletter comportant des informations actuelles. Vous pouvez révoquer la réception de cette newsletter avec effet pour le futur à tout moment, par exemple via courriel adressé à ...

Qu'en est-il avec des rappels si le destinataire ne répond pas immédiatement ?

Un courriel de confirmation (sans aucune publicité) est acceptable, mais il est toujours possible qu'un courriel de confirmation échappe à l'attention ou, dans le pire des cas, atterrisse même dans le filtre à pourriels. Est-ce qu'on peut alors, lorsque le destinataire ne clique pas sur le lien de confirmation, lui envoyer un courriel de rappel ?

Malheureusement, il n'existe pas de réponse claire et nette à cette question. Comme nous l'avons déjà constaté plus haut, il faut déjà se réjouir du fait que la cour fédérale de justice BGH a constaté que le courriel de confirmation ne constitue pas de nuisance déraisonnable. En ce qui concerne la question de savoir s'il faut considérer un courriel de rappel comme une nuisance déraisonnable, il semblerait, selon nos recherches, que la jurisprudence s'enferme à ce jour dans le mutisme. On peut cependant présumer que les tribunaux verraient d'un œil beaucoup plus critique un tel courriel de rappel, plus critique qu'un courriel de consentement. Le courriel de confirmation sert uniquement le but de vérification de l'adresse courriel et donc de l'obtention d'un consentement juridiquement sûr et infaillible. Or, le courriel de rappel sert plutôt le but d'attirer l'attention sur un défaut de confirmation et d'obtenir, peut-être, quand même le consentement, même si le destinataire ne l'avait pas confirmé à la première tentative pour quelque raison que ce soit. Il devrait donc être plus difficile de démontrer ici un intérêt légitime de l'envoi du courriel de rappel au-delà de

l'allongement de la liste de distribution. Mais ceci n'implique pas que l'envoi d'un tel courriel de confirmation est clairement illicite.

Lorsqu'on envoie un courriel de rappel, celui-ci doit toutefois toujours être envoyé une seule fois et dans un délai relativement rapproché après l'envoi du courriel de confirmation. Les courriels de rappels envoyés à des intervalles réguliers sur une période de plusieurs semaines ou de mois finiront sûrement par agacer le destinataire et par entraîner des plaintes.

Suppression des données en cas d'absence de réaction

Pendant combien de temps peut-on donc stocker les données si aucune confirmation n'est donnée ? Ici aussi, il est difficile d'indiquer une période absolue. De manière abstraite, on peut dire que les données ne peuvent être stockées que sur la seule période nécessaire à la mise en œuvre de la procédure double-opt-in.

Se pose alors la question de savoir quelle est la durée d'un tel délai raisonnable, donc, pendant quel délai on peut s'attendre à une confirmation donnée par le destinataire si on veut être réaliste. L'expérience a montré que la confirmation d'un abonnement d'une newsletter se fait dans quelques minutes. Si le destinataire est par exemple en vacances et a la chance de ne pas être joignable par courriel, il est toutefois possible que la confirmation de l'abonnement d'une newsletter faite par le destinataire ne soit donnée qu'après huit ou quinze jours. De ce fait, le droit de la protection des données considère comme encore licite un délai de quinze jours.

Fonction Tell-a-Friend

Une fonction dite Tell-a-Friend permet à un utilisateur de l'internet d'informer ses amis d'un site internet qu'il a visité. Pour ce faire, il saisit les adresses courriel de ses amis dans un formulaire directement sur le site internet et les amis reçoivent de manière automatisée un courriel comportant l'URL concerné. La question de savoir s'il s'agit alors chez les courriels envoyés de cette manière de publicité par courriel illicite faite par le fournisseur de la fonction Tell-a-Friend ou de messages privés licites envoyés par l'utilisateur de la fonction Tell-a-Friend à ses amis, prête alors à discussion.

Par son jugement du 12 septembre 2013, réf. I ZR 208/12, la cour fédérale de justice BGH a nettement limité l'utilisation de la fonction Tell-a-Friend et l'a soumise à certaines conditions préalables. La cour s'était trouvée face aux faits suivants : le demandeur avait reçu à plusieurs reprises et sans son consentement préalable des recommandations de produits de la défenderesse qui avait installé sur son site web une fonction de recommandation, la demanderesse y étant désignée (aussi) comme expéditeur des courriels de recommandation. C'est pourquoi le demandeur voulait exercer contre la défenderesse une action en cessation. Les tribunaux des instances précédentes (le tribunal d'instance et le tribunal de grande instance de Cologne) avaient rejeté cette action en invoquant le motif que le défendeur ne devait être rendu responsable des actes abusifs commis par un tiers concernant la recommandation.

La cour fédérale de justice BGH n'était toutefois pas de cet avis. Tout d'abord, elle

a qualifié les courriels de recommandation litigieux de publicité au sens de la directive 2006/113/CE (selon laquelle toute déclaration lors de l'exercice d'un commerce, d'un métier, d'un artisanat ou d'une profession libérale dans le but de stimuler les ventes de marchandises ou les prestations de services est définie comme un acte de publicité - pour ce qui est de la définition du terme publicité, cf. également sous ch. 2.2). De plus, il conviendrait toujours d'attribuer les courriels de recommandations à la responsabilité de l'exploitant du site web et ceci indépendamment de la question de savoir si c'est un tiers qui est à l'origine de ces courriels. Le point décisif serait notamment le fait que la défenderesse figurerait chez le destinataire comme étant l'expéditeur du courriel de recommandation. En fin de compte, le but de la fonction de recommandation consisterait à attirer l'attention sur le site web et les prestations de services qui y sont proposées. Ainsi, on lit dans les motifs du jugement :

« Le fait que la défenderesse ne prend pas le risque de l'abus de la fonction de recommandation ne fait pas obstacle à cette évaluation. Il est clair que la fonction de transmission est justement utilisée à envoyer des courriels de recommandation à des tiers sans être sûr si ces tiers ont déclaré leur consentement à cette transmission. »

Par conséquent, ce qui compte à un degré essentiel, dans la fonction Tell-a-Friend aussi, tout au moins lorsque l'entreprise recommandée figure également comme l'expéditeur, c'est de savoir si le destinataire a donné son consentement exprès pour la réception non sollicitée de tels contenus. Faute de consentement, il y a lieu de protéger le consommateur qui, lui, ne peut rien contre la réception de courriels de publicité non sollicités. Dans de tels cas de figure, les courriels sont illicites selon les dispositions stipulées à l'article 7, paragraphe 2, point 3 de la loi UWG.

Dans son jugement du 24 janvier 2014, réf. 5 U 42/12, le tribunal régional supérieur de Berlin a laissé transparaître que sous certaines conditions, la fonction Tell-a-Friend peut être mise à disposition en conformité avec la loi. Une condition préalable essentielle dans ce contexte est le fait que le message est présenté au destinataire comme un message privé émanant d'un ami ayant initié l'envoi, à l'exclusion de toute communication commerciale de la part du fournisseur de la fonction Tell-a-Friend. En l'espèce, la fonction incriminée était la fonction « trouver des amis » chez Facebook. Dans ce cas, des courriels invitant à l'utilisation de Facebook avaient été envoyés au nom d'un utilisateur de Facebook à toutes les adresses courriels figurant au répertoire d'adresses courriel de l'utilisateur Facebook et qui n'étaient pas encore membres chez Facebook. Contrairement au jugement ci-dessus prononcé par la cour fédérale de justice BGH le 12 septembre 2013, l'expéditeur indiqué n'était pas l'entreprise bénéficiaire de la publicité, mais l'utilisateur de Facebook. Le tribunal régional supérieur de Berlin a estimé qu'il ne s'agissait pas de publicité par courriel de la part de l'entreprise bénéficiaire de la publicité, si cette dernière se contente d'apporter une assistance technique pour l'envoi. Le tribunal estime que les courriels envoyés à l'aide de la fonction Tell-a-Friend sont imputables à l'utilisateur lorsque c'est lui qui a initié l'envoi des courriels sous sa propre

responsabilité et en toute connaissance de toutes les conditions de l'envoi. Mais dans le cas qui a été jugé par le tribunal régional supérieur de Berlin, c'était justement cette connaissance de toutes les conditions qui faisait défaut. Facebook n'avait pas clairement indiqué à l'utilisateur qu'un courriel d'invitation en son nom serait envoyé à toutes les adresses courriels figurant dans son répertoire d'adresses courriel qui n'étaient pas encore membres chez Facebook. C'est en raison de ce défaut de transparence au niveau de la conception de la fonction Tell-a-Friend que le tribunal a estimé que la responsabilité de l'envoi des courriels incombait à Facebook. La cour fédérale de justice BGH a confirmé le jugement (jugement du 14 janvier 2016, réf. I ZR 65/14), à l'heure actuelle, les motifs de la décision ne sont toutefois pas encore disponibles, de sorte qu'il n'est pas clair si la cour fédérale de justice BGH a traité en plus de détail la question de la licéité fondamentale de la fonction Tell-a-Friend.

2.11 Documentation du consentement

Indépendamment de la procédure utilisée, il y a lieu de documenter intégralement et dans la pérennité la déclaration de consentement pour toute la durée d'utilisation de l'adresse courriel, des prescriptions de justification stipulées par la cour fédérale de justice BGH (jugement du 10 février 2011, I ZR 164/09) devant être prises en compte lors de la consignation. En cas de litige, l'expéditeur d'un courrier de publicité doit être en mesure de fournir au moins les détails suivants :

- le contenu de la déclaration de consentement et les informations relatives à la conception (comment est-ce que le consentement a été déclaré : activement ou séparément ?) ;
- la date de la déclaration de consentement ;
- l'adresse IP de la personne consentante à la date du consentement (pour les adresses IP dynamiques, la valeur probante de l'adresse IP est bien entendu très limitée) ;
- le cas échéant, la date d'envoi du courriel d'invitation (pour un double-opt-in) ;
- le contenu du courriel d'invitation (pour un double-opt-in) ;
- la date de la confirmation du consentement (pour un double-opt-in).

Dans le cas d'un consentement déclaré à l'occasion d'un contact personnel, il est éventuellement possible de recourir, en complément à la confirmation écrite, au destinataire de la déclaration en tant que témoin. La déclaration de ce dernier doit, dans l'éventualité d'un litige (devant les tribunaux), être considéré comme crédible. Celle-ci est mise en doute lorsque le contact date d'il y a longtemps et s'il a eu lieu dans le cadre d'une multitude de contacts, comme par exemple à l'occasion d'un salon. Par ailleurs, il n'est pas non plus sûr que le contact soit réellement la personne recevant ultérieurement la publicité. Ici aussi, la réalisation d'une procédure double-opt-in - adaptée en conséquence - serait utile.

2.12 Exception de l'opt-in : publicité par courriel par une relation client déjà en place

Dans le cadre de relations clients déjà en place, le législateur prévoit un allègement pour la publicité par courriel à l'article 7, paragraphe 3 de la loi UWG. Normalement, le publicitaire doit disposer de l'autorisation

consciente et indubitable du destinataire afin de pouvoir lui envoyer des courriels de publicité (autorisation appelée opt-in). Or, pour une relation client déjà en place, il est possible d'envoyer des courriels de publicité au client si le client ne s'est pas opposé à ces envois (opposition appelée opt-out). Ce régime d'exception prévoit toutefois certaines conditions préalables formelles, raison pour laquelle on parle également d' « Opt-Out [1] ». Plus exactement, ces conditions préalables se présentent comme suit :

- l'expéditeur doit avoir obtenu l'adresse courriel du client « par le client dans le contexte de la vente d'une marchandise ou d'une prestation de services » ;
- de plus, il faudrait que le client « en ait été clairement et indubitablement informé lors de la collecte de l'adresse et lors de chaque utilisation » de ce qu'il peut s'opposer à tout moment de l'utilisation de son adresse courriel à des fins publicitaires ;
- *« sans que ceci n'engendre d'autres frais que ceux de transfert selon les tarifs de base »* – et que le client ne s'y est pas opposé, bien entendu ;
- dans les courriels envoyés au client par la suite, il est admissible de faire de la publicité exclusivement pour « ses propres marchandises ou prestations de services similaires ».

La loi stipule expressément que le client doit lui-même indiquer son adresse courriel au publicitaire dans le cadre du traitement de la commande. Par conséquent, le fait pour le publicitaire d'avoir obtenu ou découvert l'adresse courriel du client par d'autres moyens, ne suffit pas.

La question de savoir si le processus de vente doit effectivement avoir été terminé afin d'être en droit d'exploiter l'adresse courriel pour de la publicité par courriel fait l'objet de tous les débats. Cette question devient pertinente par exemple en cas de demande de la part de clients potentiels et dans des boutiques en ligne pour les clients d'une boutique qui, au cours du processus de leur commande, posent de la marchandise dans le panier et indiquent leur adresse courriel, mais qui ensuite annulent le processus de commande. Est-ce que, dans de tels cas, la prescription réglementaire stipulant « le contexte de la vente » est déjà remplie ou est-ce que le contrat doit effectivement avoir été conclu ?

Alors qu'il n'est pas contesté dans beaucoup d'autres pays européens qu'il suffit de négocier des contrats afin de pouvoir se réclamer de ce régime d'exception, il n'existe toujours pas de consensus à ce sujet en Allemagne. D'un côté, il y a les partisans d'une protection la plus étendue possible contre toute publicité excédante par courriel qui prêchent une interprétation stricte du régime d'exception et considèrent comme obligatoire la conclusion d'un processus de vente. Le libellé de l'article 7, paragraphe 3 de la loi UWG qui évoque explicitement le CLIENT, joue en faveur de ces partisans. D'un autre côté, on fait valoir qu'un prospect qui a fourni son adresse courriel volontairement dans le cadre du processus de la commande et qui a été informé de ce qu'il recevra à l'avenir de la publicité par courriel, sauf pour lui de s'y opposer, ne nécessiterait pas de protection particulière.

1 *`Comme déjà expliqué, en Allemagne c'est toujours la procédure opt-in qui est valable. C'est uniquement lorsque les conditions préalables strictes stipulées à l'article 7, III sont remplies, que l'on parle exceptionnellement d'un opt-out dit « qualifié » ou d'un soft-opt in.*

L'exploitation des adresses courriel qui ont été collectées « dans le cadre de la vente d'une marchandise ou d'une prestation de service » comporte donc un risque juridique résiduel si cette vente n'a pas été complétée intégralement. Un jugement de dernière instance apportant une réponse définitive à cette question n'existe pas (semble-t-il).

Afin de tomber dans le champ d'application du régime d'exception de l'article 7, paragraphe 3 de la loi UWG, il doit s'agir d'un acte juridique conclu à titre onéreux. Dans le cas d'une prestation de services rendue à titre gracieux, comme par exemple l'affiliation gratuite à une plateforme d'internet, les conditions préalables de l'article 7, paragraphe 3 de la loi UWG ne sont pas remplies.

Une transmission de l'adresse courriel à d'autres entreprises, même du même groupe, est exclue de toutes les manières. Une exploitation de l'adresse à des fins publicitaires au profit d'autres entreprises est également illicite.

Par ailleurs, le publicitaire peut envoyer au client uniquement de la publicité par courriel concernant « ses propres marchandises et prestations de services similaires ». Ici se pose alors la question de savoir ce qu'il y a lieu d'entendre par cette formule abstraite. La similitude requise entre la marchandise acquise et les marchandises pour lesquelles une publicité ultérieure est licite est définie du point de vue du client. En se basant sur les achats du passé, le publicitaire doit se poser la question de savoir quelles autres marchandises similaires le client pourrait éventuellement trouver intéressantes aussi.

Selon la jurisprudence, la similitude entre les marchandises se détermine en fonction du but d'utilisation typique de la marchandise objet de la publicité ou de la conformité au besoin du client avec la marchandise déjà achetée dans le passé. Lorsque les deux marchandises servent au même but d'utilisation, il y a similitude. Dans ce contexte, même les accessoires et les marchandises de complément sont toujours reconnues par la jurisprudence comme étant « similaires », même si la jurisprudence se base, en principe, sur une interprétation stricte du régime d'exception.
Si par exemple un client commande du vin rouge français, il s'intéressera certainement aussi aux vins en provenance d'Autriche ou d'autres pays - on est alors en droit de l'en informer. Les informations relatives aux accessoires de la marchandise acquise à l'origine devraient, elles aussi, tomber sans problèmes sous le régime d'exception. C'est pourquoi, les commerçants spécialisés en ligne qui proposent uniquement des marchandises faisant partie d'un segment spécifique pourront donc mieux exploiter le régime d'exception qu'un vendeur par correspondance proposant une large gamme de marchandises et qui fait de la publicité non spécifique pour des marchandises de toutes les gammes dans sa newsletter.

Lorsque le publicitaire utilise, dans le cadre de sa boutique en ligne, un « opt-in actif » où le client doit cliquer sur une case à cocher afin de recevoir la newsletter à l'avenir, il peut exceptionnellement intégrer cette case à cocher « déjà cochée » dans son processus de commande quand il s'agit de l'envoi de ses propres produits similaires dans le cadre des relations clients exposées ci-dessus. Ce faisant, il y a lieu de toujours rappeler la

faculté de s'opposer à tout moment à l'envoi de courriels de publicité sans que ceci ne génère d'autres coûts de transmission que ceux générés par le tarif de base.

Dans ce cas, l'utilisateur doit devenir actif et « désactiver » la case à cocher s'il ne souhaite pas recevoir de courriels de publicité portant sur les produits propres et similaires du publicitaire. L'expérience a montré qu'un tel changement permet de générer au moins un redoublement de la conversion. Bien entendu, le publicitaire devra alors respecter la restriction de la publicité à « ses propres marchandises et prestations de services similaires ». S'il souhaite exploiter les adresses obtenues de cette manière pour l'envoi de newsletters, celle-ci ne doit faire de la publicité que pour des marchandises de la même espèce.

Une conversion nettement plus élevée serait certainement obtenue par un tour-opérateur qui intègre dans son processus de commande le texte suivant :

Nous vous envoyons votre confirmation de réservation à l'adresse courriel que vous nous avez indiquée. De plus, nous vous joignons dans le contexte de votre réservation, en complément à votre confirmation de réservation, des courriels supplémentaires comportant des informations et des offres susceptibles de vous intéresser dans le cadre de votre voyage. Vous pouvez vous opposer à tout moment à cet envoi en adressant un courriel à ubsubscribe@xyz.de sans que cette opposition ne génère d'autres frais de transmission que celles correspondant aux tarifs de base. Après la réception de votre opposition, nous arrêterons nos envois par retour.

Cette conception garantit une conversion de pratiquement cent pour cent, toutefois, le contenu de la communication et de la publicité suivante doit alors se restreindre absolument aux informations limitées au seul voyage effectivement réservé. Par ailleurs, il y a lieu de veiller à ce que la publicité concerne uniquement « ses propres produits ».

L'information portant sur le droit d'opposition doit suivre directement au moment de la collecte de l'adresse courriel, donc au moment où le client fournit son adresse courriel au publicitaire. Par conséquent, les clients existants dont l'attention n'avait pas été attirée sur leur droit d'opposition au moment de la divulgation de leur adresse courriel, ne sauraient en être informés tout simplement par un courriel envoyé à posteriori. Il conviendrait plutôt de les persuader d'indiquer leur adresse courriel encore une fois et alors attirer leur attention sur leur droit d'opposition à cette occasion. À cet effet, on peut par exemple proposer au client une prestation complémentaire a posteriori (en cas de besoin, à titre gratuit) nécessitant l'indication de l'adresse courriel pour passer commande. Cette qualification a posteriori est toutefois rendue plus difficile par le fait qu'il est interdit d'attirer l'attention des clients existants aux prestations complémentaires par l'envoi de courriels. Ici, il y a lieu de choisir des moyens alternatifs de la prise de contact, comme par exemple via le site web, par courrier ou dans le cadre de mailings de transactions.

2.13 La publicité dans les courriels de transactions

Les courriels de transactions sont des courriels qu'une entreprise envoie dans le cadre de l'exécution d'un contrat, comme par exemple les confirmations de commande, les avis d'expédition ou les factures. Bien entendu, aucun consentement de la part du destinataire n'est nécessaire à l'expéditeur de tels courriels de transactions. Du point de vue du marketing, il serait utile de combiner par la même occasion de tels courriels de transactions avec d'autres produits et prestations de services proposés par le publicitaire, étant donné que la publicité contenue dans des courriels de transactions présente une conversion hors pair.

La grande question qui se pose dans ce contexte est de savoir si les courriels de transaction peuvent comporter de la publicité alors que le destinataire n'a pas consenti à la réception de courriels de publicité et lorsque les conditions préalables pour l'exception valable pour le marketing par courriel dans des relations clients déjà en place (cf. 2.12) ne sont pas remplies.

L'envoi de courriels de publicité nécessite le consentement du destinataire, car on souhaite éviter « une nuisance déraisonnable » occasionnée par une publicité de masse non sollicitée. Selon l'avis du législateur, la « nuisance déraisonnable » consiste dans le fait que le destinataire est obligé de lire chacun des courriels qu'il a reçus et ainsi, tant qu'il s'agit de publicité non sollicitée, de la supprimer. Mais un courriel de transaction ne saurait constituer une telle « nuisance déraisonnable ». Le destinataire reçoit le courriel de transaction, donc par exemple l'avis d'expédition, dans tous les cas de figure et doit le lire, ceci indépendamment de la question de savoir si celui-ci est oui ou non assorti de contenus publicitaires.

Or, si les courriels de transactions cachent de la publicité, même si celle-ci n'est qu'accessoire, ce n'est pas la même chose. C'est au plus tard lorsque le destinataire de la publicité s'y est expressément opposé que l'envoi de publicité contenue dans des courriels de transactions, a priori admissibles, est dans tous les cas de figure illicite. Dans ce contexte, la cour fédérale de justice BGH, dans son jugement du 15 décembre 2015, réf. VI ZR 134/15, a décidé que la publicité contenue dans un courriel de réponse automatique, comme par exemple la confirmation automatisée de la réception d'un courriel, est illicite lorsque le destinataire s'était expressément opposé à la réception de publicité par courriel au préalable. Dans l'affaire en question, le demandeur avait résilié par courriel le contrat qu'il avait conclu auprès de la compagnie d'assurance défenderesse. En réponse, il a reçu un accusé de réception automatisée par courriel qui contenait, à sa fin, une indication succincte sur un service d'avertissement d'intempéries proposé par l'assurance. Sur ce, le demandeur s'est adressé de nouveau à l'assurance par courriel en expliquant explicitement ne pas consentir à l'envoi de la publicité contenue dans l'accusé de réception automatisée. En réponse à ce courriel ainsi qu'à un autre courriel comportant une demande de l'état d'avancement de l'affaire envoyé une semaine plus tard, il a de nouveau reçu un accusé de réception automatisée comportant, lui aussi, l'indication sur le service d'avertissement d'intempéries.

La cour fédérale de justice BGH a décidé dans cette affaire que tout au moins le dernier courriel d'accusé de réception envoyé par la compagnie d'assurance était illicite.[2] D'une part, l'indication sur le service d'avertissement d'intempéries constituait, selon l'avis de la cour fédérale, de la publicité (pour ce qui est de la définition du terme publicité, cf. également sous ch. 2.2 ci-dessus). Et d'autre part, cette publicité a été envoyée contre la volonté exprimée explicitement par le destinataire - et constituait ainsi pour le destinataire une nuisance déraisonnable.

2.14 Demande de retour d'expérience après l'achat

Pour beaucoup d'entreprises, le retour d'expérience des clients est extrêmement précieux afin de perfectionner leur offre et de l'adapter aux besoins du marché. En plus, les évaluations de clients servent de plus en plus de base pour une décision d'achat des clients. C'est pourquoi de plus en plus de fournisseurs envoient des courriels après la conclusion d'un achat en sollicitant une évaluation ou un retour d'expérience de la part du client.

Mais est-ce que de telles demandes de retour d'expérience après l'achat sont-elles licites alors que le destinataire n'a pas consenti à la réception de courriels de publicité et lorsque les conditions préalables pour l'exception valable pour le marketing par courriel dans des relations clients déjà en place (cf. ci-dessus) ne sont pas remplies ?

La question décisive est de savoir si de telles demandes de retour d'expérience constituent de la publicité. Le tribunal de grande instance de Coburg y a répondu par la négative (jugement du 17 février 2012, réf. 33 S 87/11). Selon ce jugement, une seule et unique demande de retour d'expérience envoyée par courriel ne constituerait pas de publicité, mais serait avant tout du « service après-vente devant servir au perfectionnement des processus et à l'élimination de défauts ». Par ailleurs, les demandes de retour d'expérience seraient devenues monnaie courante de nos jours. Par conséquent, le tribunal n'a pas estimé nécessaire le consentement du destinataire à la réception de la publicité. Ce jugement a fait l'objet de fortes critiques, en partie avec de bons arguments. Il n'est pas du tout sûr non plus que d'autres tribunaux décideraient de la même manière. De ce fait, il convient de respecter les exigences formelles de l'exception valable pour le marketing par courriel avec les relations clients déjà en place (cf. ci-dessus) pour éviter d'emblée tout problème juridique.

2 *Explication succincte : ici, la cour fédérale de justice BGH se référait à la base de revendication en vertu des articles 1004 et 823 du code civil allemand (Bürgerliches Gesetzbuch, BGB), étant donné que le demandeur en tant que personne physique ne pouvait revendiquer des droits résultant de la loi UWG. Dans son jugement, la cour constate que toute publicité sans consentement constitue une nuisance déraisonnable (UWG). Malheureusement, la cour ne précise pas dans quelle mesure une violation de l'article 13 EU-DS_RiLi est pertinente dans le cadre de l'article 823 du BGB. Or, il ne faut pas en tirer la conclusion selon laquelle une publicité contenue dans des courriels de transaction ne poserait pas de problèmes en l'absence d'une opposition.*

2.15 Conséquences juridiques en cas de non-respect des prescriptions légales

Dans le cas d'un litige devant les tribunaux concernant la licéité de l'envoi de courriels de publicité, la charge de la preuve et de l'allégation de la fourniture effective du consentement donné par le titulaire en question de l'adresse courriel utilisé incombe à l'expéditeur au sens de l'article 13, paragraphe 2 de la loi TMG, article 7, paragraphe 2, point 3 de la loi UWG, article 28, paragraphe 3, lettre a) de la loi BDSG. La seule allégation selon laquelle un consentement à la réception de courriels de publicité a été fourni à une adresse courriel spécifique ne saurait suffire lorsque l'expéditeur n'est pas en mesure de prouver que le consentement provient effectivement du titulaire de l'adresse courriel utilisé. Les conditions préalables minimum sont le texte de consentement au moment de la collecte des données, la date et l'heure ainsi que la source du consentement (cf. chapitre 2.11).

À l'heure actuelle, les destinataires se défendant contre la réception de courriels de publicité non sollicités sont de plus en plus nombreux. Ainsi, le bureau des plaintes eco a reçu en 2015 plus de 190 000 plaintes émanant d'utilisateurs et portant sur des courriels.

Certes, les litiges devant les tribunaux ayant pour objet la licéité de l'envoi de courriels de publicité ne sont pas très fréquents, car en règle générale les parties tentent de s'arranger à l'amiable. Même une procédure extra-judiciaire génère des coûts, mais contrairement à une procédure devant les tribunaux, ces coûts restent raisonnables. Ceux-ci englobent par exemple des frais d'avis formels et les honoraires d'avocats ainsi que les demandes en dommages-intérêts.

Dans l'éventualité d'une procédure devant les tribunaux, l'expéditeur des courriels de publicité doit s'attendre à des frais élevés s'il venait à perdre le procès.

Les frais de procédure sont fonction de la valeur du litige en question qui, elle, est déterminée par le juge compétent. La valeur du litige peut être comprise entre 100 euros et plus de 30 000 euros (BGH I ZR 38/10) et varier en fonction de chaque affaire et de l'instance du tribunal. Une valeur du litige de 30 000 euros est susceptible de générer pour l'expéditeur des frais d'avocat, des frais de justice ainsi que des dommages-intérêts s'élevant au total à un montant de plus de 5 000 euros. Alors, lorsque par exemple quatre destinataires de courriels de publicité non sollicités intentent une action en justice contre l'expéditeur, ce dernier risque de subir des frais pouvant atteindre 20 000 euros. En plus, les expéditeurs de courriels de publicité illicites sont susceptibles d'être jugés en cessation des actes illicites. Dans un tel cas de figure, les tribunaux prévoient en complément une amende civile pouvant atteindre 250 000 euros pour chaque cas de contravention si le demandeur en fait la demande.

C'est pourquoi nous recommandons de respecter toutes les conditions préalables pour un envoi dans les règles de courriels de publicité afin de ne pas s'exposer à des frais de justice élevés et les demandes en dommages-intérêts.

3. La révocation

3.1 Est-ce qu'il est possible de révoquer sans problèmes son consentement à la réception de courriels de publicité ?

Toute personne envoyant des courriels de publicité est tenue à accorder au destinataire la possibilité de supprimer ses coordonnées de la liste de distribution et de clairement rappeler cette possibilité (article 28, paragraphe 4 de la loi BDSG, article 7, paragraphe 2, point 4 de la loi UWG, article 13, paragraphe 2, point 4 de la loi TMG, article 13, paragraphe 3 de la loi TMG). La meilleure variante est un lien de révocation directement dans le courriel. Après le clic, la suppression doit avoir lieu dans les meilleurs délais.

L'information quant à la possibilité de révocation doit être donnée au moment même de la demande du consentement.

Le législateur exige que le prestataire de services accorde à l'utilisateur la possibilité de révoquer à tout moment son consentement à l'exploitation de ses données voire de son opt-in (article 13 de la loi TMG, article 28, paragraphe 4 de la loi BDSG). Par ailleurs, le législateur demande explicitement que l'indication de ce droit doit impérativement être fournie à l'utilisateur avant sa déclaration du consentement (article 13, paragraphe 3 de la loi TMG).

Par conséquent, il ne suffit pas d'insérer cette indication sous forme d'un lien dans une newsletter. C'est au moment de l'enregistrement déjà que le législateur exige une information y afférente.

À première vue, cette formalité semble être anodine voire même évidente. Ceci d'autant plus que cette prescription soulage aussi l'utilisateur de la crainte de fournir son consentement « à vie ». Et pourtant – il y a peu d'entreprises qui arrivent à répondre à cette exigence du législateur.

Étant donné qu'une telle information crée aussi de la confiance, mieux vaut saisir cette chance et rassurer le destinataire de ce qu'il peut révoquer son consentement à tout moment (moyennant un simple clic de la souris).

Exemples de libellé :

- Vous pouvez révoquer votre consentement à la réception de la newsletter à tout moment avec effet pour le futur, il suffit d'un seul clic de la souris.
- Dans chaque newsletter, nous vous offrons la possibilité de résilier votre abonnement.
- Chaque newsletter comporte un lien de résiliation vous permettant de vous désinscrire de la liste de distribution à tout moment par un simple clic de la souris.
- Vous pouvez vous opposer à l'exploitation de vos données à des fins publicitaires à tout moment.

L'opposition à la poursuite du traitement ou de l'exploitation des coordonnées d'un utilisateur à des fins publicitaires doit être prise en compte par l'entreprise concernée immédiatement, cf. art. 28, al. 4, phrase 1ère de la loi BDSG.

La possibilité de résiliation doit être donnée dans chaque courriel de publicité.

La loi stipule que chaque courriel de publicité doit offrir la possibilité de se désinscrire et y attirer l'attention (article 7, paragraphe 2, point 4 de la loi UWG, article 7, paragraphe 3 de la loi UWG, article 13, paragraphe 2, point 4 de la loi TMG et article 28, paragraphe 4 de la loi BDSG).

L'article 28, paragraphe 4 de la loi BDSG stipule : *Lorsque l'utilisateur s'oppose au traitement ou à l'exploitation de ses données aux fins publicitaires ou de recherche du marché ou d'analyses de sondages auprès du service responsable, tout traitement ou toute exploitation à ces fins serait illicite. Il y a lieu d'informer l'utilisateur au moment de la prise de contact aux fins publicitaires [...] par le service responsable ainsi que de son droit d'opposition [...] ;*

Cela signifie : l'attention du (futur) destinataire doit avoir été attirée sur son droit d'opposition. Dès qu'il indique ne plus souhaiter recevoir de courriels par l'entreprise expéditrice, il y a lieu de s'assurer qu'il sera exclu de la liste de mailings futurs. Toute violation de cette opposition selon l'article 28, paragraphe 4 de la loi BDSG est susceptible d'entrainer une amende pouvant atteindre 300 000 euros (article 43, paragraphe 2, point 5, lettre b) de la loi BDSG, article 43, paragraphe 3 de la loi BDSG).

Il existe plusieurs possibilités d'informer le destinataire de son droit d'opposition. Or, toutes ces possibilités ne sont pas recommandables.

Le meilleur et le moyen le plus agréable pour l'utilisateur est un lien de résiliation contenu dans chaque courriel. Dans la plupart des cas, ce lien se trouve en bas, à la fin du courriel.

Un exemple :
Si vous ne souhaitez plus recevoir notre newsletter, il vous suffit de cliquer ici : Désabonner la newsletter

Toute solution professionnelle de courriel aux fins de marketing assure que tout utilisateur cliquant sur ce lien ne reçoit automatiquement plus de courriels.

Après le clic sur le lien, l'utilisateur doit arriver à une page confirmant la suppression de son adresse de la liste de distribution.

Exemple de libellé :
Nous vous avons retiré de notre liste de distribution. Vous ne recevrez plus aucun courriel de notre part.

Il n'est pas nécessaire de confirmer à l'utilisateur son désabonnement par courriel. Au contraire, ce courriel supplémentaire risquerait d'être considéré par l'utilisateur comme une nuisance déraisonnable étant donné qu'il vient de retirer sa permission à l'entreprise publicitaire pour lui envoyer davantage de courriels.

Ce qu'il ne faudrait utiliser en aucun cas, ce sont des processus rendant plus difficile le désabonnement de l'utilisateur, comme par exemple le « double opt-out » où l'utilisateur reçoit, après sa résiliation, un courriel l'invitant à confirmer son désabonnement en cliquant sur un lien.

L'expérience a montré qu'un pourcentage non négligeable des utilisateurs ne clique pas sur ce lien. Il est possible que ce soit justement ce courriel qui, par erreur, atterrisse au filtre à pourriels ou que l'utilisateur prenne ce courriel pour une simple confirmation de

désabonnement, sans le lire dans le détail - les raisons possibles en sont multiples. Ce qui est sûr, pourtant, c'est que l'utilisateur continuera à recevoir la newsletter en question dans un tel cas de figure. Ceci entraîne très rapidement de l'agacement – ce n'est pas vraiment ce que l'on cherche à obtenir réellement avec une newsletter.

Certaines solutions de courriels aux fins de marketing n'offrent pas l'emploi de liens de désabonnement automatique. Ici, la résiliation se fait par courriel. Il existe deux variantes courantes.

Exemple variante 1 :
Afin de vous désabonner de notre newsletter, veuillez répondre au présent courriel en mentionnant dans la ligne d'objet le mot « désabonnement ».

Exemple variante 2 :
Si vous ne souhaitez plus recevoir de courriels de nos services, veuillez envoyer un courriel vierge à unsubscribe-635094235835@firmenname.de

Dans les deux cas de figure, la solution de courriel aux fins de marketing analyse les courriels reçus et retire l'adresse du destinataire de la liste de distribution.

Les désabonnements par courriel sont également utilisés pour le désabonnement dit « list-unsubscribe ». Malheureusement, ce n'est pas encore devenu la norme et de ce fait, rares sont les logiciels de courriel et de messageries web à proposer déjà ce service complémentaire à leurs utilisateurs. Le fonctionnement en est assez simple. L'expéditeur ne se contente pas d'intégrer le lien de désabonnement au contenu de sa newsletter, mais également dans l'en-tête du courriel. Ensuite, le logiciel de courriel voire la messagerie web met à disposition un bouton dédié permettant le désabonnement. Lorsque le destinataire clique sur ce bouton, le système envoie à l'arrière-plan automatiquement un courriel à une adresse courriel prévue à cet effet et le désabonnement est réalisé. L'avantage de cette variante : le bouton de désabonnement a un emplacement fixe dans le logiciel de courriel et vaut pour les newsletters de tous les expéditeurs qui supportent la méthode « list-unsubscribe ». Il n´est donc pas nécessaire de chercher le lien de désabonnement dans la newsletter.

En complément, il y a lieu de prévoir la possibilité de traiter correctement même les abonnements via d'autres voies. Donc, lorsqu'un utilisateur envoie un courriel informel dans lequel il demande son désabonnement, il faut garantir que cette demande soit lue et traitée dans les meilleurs délais.

Ceux qui sont en contact avec leurs clients via un centre d'appels ou bien un service en ligne doivent garantir que même les désabonnements reçus par téléphone dans ces services soient traités rapidement sans « tomber dans les oubliettes ».

La variante où le site web propose, en plus du formulaire d'inscription, également un formulaire de désabonnement dans lequel l'utilisateur inscrit son adresse courriel (cette variante étant tout au plus appropriée en tant que complément) n´est pas recommandable. La raison : nombreux sont les utilisateurs à faire dérouter leurs courriels venant d'un autre compte courriel sur leur adresse courriel préférée et en cas de doute,

ils ne savent plus avec laquelle de leurs différentes adresses courriels ils se sont inscrits. Par conséquent, certains utilisateurs ne seront plus en mesure de se désabonner, ce qui présente un risque de frustration.

Mais il y a pire encore.

Worst Practice/exemple négatif

Pour vous désabonner de la newsletter xyz, veuillez-vous connecter sous www.xyz.de à l'aide de votre identifiant et de votre mot de passe. Rendez-vous ensuite à la zone « mon profil » et décochez « newsletter » dans la zone « configuration courriel ».

Une telle manière de procéder est, premièrement, compliquée et, deuxièmement, il est plus que probable qu'un pourcentage non négligeable des utilisateurs aura déjà oublié ses données d'enregistrement d'origine depuis belle lurette.

Liste de vérification

- ✔ Est-ce que l'attention a été attirée à la possibilité de désabonnement avant la réception du consentement ?
  ☐ Oui / ☐ Non
- ✔ Est-ce que l'attention est attirée sur la possibilité de désabonnement dans tous les formulaires en ligne / hors ligne ?
  ☐ Oui / ☐ Non
- ✔ Est-ce que chaque courriel de publicité comporte une possibilité de désabonnement ?
  ☐ Oui / ☐ Non
- ✔ Est-ce qu'il est possible de se désabonner sans détour (sans double-opt-out ou bien connexion obligatoire ?)
  ☐ Oui / ☐ Non
- ✔ Est-ce que l'adresse est supprimée rapidement de la liste de distribution après le désabonnement ?
  ☐ Oui / ☐ Non
- ✔ Est-ce qu'il est garanti que même les désabonnements entrant par d'autres canaux sont traités dans les meilleurs délais ?
  ☐ Oui / ☐ Non

3.2 Réagit-on aux demandes et aux réclamations ?

La publicité par courriel, c'est du marketing de dialogue. C'est pourquoi il est particulièrement important de répondre rapidement aux demandes et aux réclamations. C'est justement parce que le marketing par courriel est un médium tellement rapide que l'on ne doit pas se permettre de négligence ici. Un délai de 24 heures est habituel.

Les personnes qui se plaignent ou fournissent un retour d'expérience ont toujours un grand intérêt dans l'entreprise :

- si elles sont correctement prises en charge et traitées, les réclamations peuvent même être inversées (objectif : un client satisfait) ;
- les retours d'expérience, de quelque type que ce soit, servent aussi toujours à un processus de perfectionnement - qu'est-ce qui va bien dans l'entreprise, qu'est-ce qui va mal;
- les retours d'expérience peuvent ouvrir la voie à des affaires concrètes : c'est surtout pour les courriels que beaucoup de personnes sont habituées à se contenter de cliquer sur « répondre ». Une entreprise ne devrait pas se priver de cette chance de dialogue.

Les retours aux courriels sont reçus dans une entreprise par plusieurs voies :

1. chaque envoi de courriels génère des retours - des avis d'absence et autres réponses automatisées (p. ex. « j'ai changé de service, désormais, ce service est assuré par Monsieur Dupont) message d'impossibilité de livraison, confirmations de réception, de « vraies » réponses, etc. ;
2. des « vraies » réponses reçues via l'adresse courriel d'assistance publiée ;
3. des réponses par d'autres voies, comme le téléphone, le fax, le courrier ou l'avocat.

Pratiquement toutes les solutions modernes de courriels aux fins de marketing filtrent les avis d'absence, les retours, etc. automatiquement pour traiter ces courriels (p. ex., les retours sont bloqués pour tout envoi ultérieur). Le défi dans ce cas consiste à tamiser les « vrais » retours. Ceci peut se faire soit manuellement, soit automatiquement. Le contenu de la boîte à lettres destinée pour l'adresse « reply-to » (réponse à) ne peut en aucun cas être supprimé.

On peut alors traiter les « vraies » réponses ainsi filtrées, tout comme les réponses entrant via les adresses courriel d'assistance normales.

Les modules de textes fournissant des réponses aux questions standards courantes conviennent très bien à cet effet. Afin de permettre un traitement des processus de réponses à parfois plusieurs dizaines de milliers de courriels dans un laps de temps très court, il existe des systèmes de gestion de réponses spécifiques. La question de savoir s'il convient alors de préférer les systèmes entièrement automatisés munis d'une « intelligence artificielle » ou plutôt des « systèmes basés sur des règles » assistant, certes, les agents des centres d'appels sans pour autant les remplacer, est alors une question de foi. En règle générale, les réactions des clients sont plutôt l'agacement lorsqu'ils reçoivent une réponse (visiblement) générée par des dispositifs automatiques. Plus le sujet de la question est traité de manière précise, plus il est probable que le client sera satisfait.

Dans des cas rares, les destinataires appellent. Ce qui compte dans un tel cas, c'est que les agents du centre d'appel aient accès aux bases de données de courriel pour être en mesure de répondre au moins aux questions les plus importantes de manière exhaustive (« D'où tenez-vous mon adresse ? », « Ne m'envoyez plus de courriels ! »)

Le point décisif dans les deux cas (le retour électronique tout comme les réponses par les autres voies), c'est que les processus pour les réponses et les réclamations soient définis et documentés. Une importance particulière revient à la rapidité de la réponse - pour le médium rapide qu'est le courriel, l'attente est de 24 heures au maximum.

Liste de vérification :

- ✔ Est-ce que le courriel indique une adresse d'assistance à laquelle on peut s'adresser par courriel ou par téléphone ?
  ☐ Oui / ☐ Non
- ✔ Est-ce qu'il est garanti que l'adresse d'expédition / « reply-to » fonctionne et que les messages qui y sont adressés ne sont pas perdus ?
  ☐ Oui / ☐ Non
- ✔ Est-ce que des retours de courriels à l'adresse d'expédition sont filtrés automatiquement et corrigés des retours / avis d'absence ?
  ☐ Oui / ☐ Non
- ✔ Est-ce que les « vrais » retours de courriels sont de manière permanente contrôlés, soit par un système muni d'une intelligence artificielle, soit par un collaborateur, et est-ce qu'on y répond directement ou est-ce qu'on les transmet aux services correspondants ?
  ☐ Oui / ☐ Non
- ✔ Est-ce que le centre d'appels peut accéder à la base de données des courriels, p. ex. afin de pouvoir bloquer des adresses immédiatement ?
  ☐ Oui / ☐ Non
- ✔ Est-ce que le centre d'appels est informé des courriels sortants ?
  ☐ Oui / ☐ Non
- ✔ Existe-t-il des listes de vérification et des procédures stipulant la manière de procéder dans des cas « critiques » ?
  ☐ Oui / ☐ Non
- ✔ Est-ce que les délais de réponses et la satisfaction avec la qualité / les réponses sont analysés?
  ☐ Oui / ☐ Non
- ✔ Est-ce qu'il est répondu rapidement aux demandes / réclamations (le délai courant étant de 24 heures) ?
  ☐ Oui / ☐ Non

4. Conception de la newsletter

La conception de la newsletter elle-même requiert, elle aussi, le respect de certaines prescriptions légales.

4.1 Objet

La communication commerciale via courriel doit toujours être clairement marquée comme telle (article 6, paragraphe 2 de la loi TMG). Par conséquent, l'objet de la newsletter ne doit pas dissimuler qu'il s'agit d'un courriel servant à des fins publicitaires. Il y a dissimulation de ce type si l'expéditeur a volontairement conçu l'objet de son courriel de sorte que le destinataire est induit en erreur sur le caractère commercial du courriel.

La motivation de la loi cite les exemples suivants pour des lignes d'objet induisant en erreur :

- « Dernier avertissement »
- « Attention, très urgent ! »
- « Votre procédure pénale, référence XY »

Le but poursuivi par de telles lignes d'objet c'est qu'un maximum possible de destinataires ouvre le courriel. Mais il y a lieu de protéger les destinataires de l'obligation d'ouvrir des courriels afin de découvrir si le courriel comporte des contenus pertinents. Il faut au contraire que le destinataire se rende compte à la lecture de l'objet déjà qu'il s'agit d'une newsletter comportant de la publicité. Cela ne signifie pas pour autant que le terme « newsletter » doit forcément être indiqué dans l'objet. Le caractère commercial d'un courriel de publicité est visible même dans d'autres libellés typiques pour la publicité.

Exemples :
- « Vos propositions de la semaine »
- « Une offre limitée d'ici dimanche - 20 % de remise sur toute la gamme »
- « Achetez maintenant la mode du printemps premier prix »

Du point de vue du marketing, l'objet de la newsletter doit être aussi succinct, précis et attractif que possible. Afin de s'adresser au destinataire de la newsletter de manière encore plus personnalisée, il est également utile de prévoir un objet personnalisé de la newsletter.

De plus, il ne faut pas oublier non plus que l'objet de courriels faisant partie du marketing par courriel est vérifié par les filtres à pourriels. C'est pourquoi, il convient d'éviter tous les termes et formules risquant de faire atterrir la newsletter dans le registre à pourriels.

Exemples :
- Signes spéciaux (p. ex. $!?)
- MAJUSCULES SUR TOUTE LA LIGNE
- Sans frais, gratuit, garantie
- Commandez aujourd'hui ! Commandez maintenant !
- Garantie de remboursement
- Poker, casino, chance de gagner

Les filtres à pourriels changent tout le temps afin de s'adapter même aux vagues de pourriels les plus récentes. C'est pourquoi il est recommandé aux expéditeurs de newsletters de vérifier, en cas de doute, à travers des tests si leur newsletter risque d'être filtrée par les filtres à pourriels courants. Il y a des prestataires de services permettant de vérifier gratuitement si la newsletter est classée comme pourriel.

4.2 Contenu

Le contenu de la newsletter doit, lui aussi, être clairement marqué comme étant à caractère commercial (article 6, paragraphe 1, point 1 de la loi TMG). De plus, le destinataire doit être identifiable (cf. à ce sujet 4.3). Si la newsletter présente des offres spécifiques relatives à la promotion des ventes (comme par exemple des réductions des prix, des primes ou des cadeaux), les conditions pour leur obtention doivent être facilement accessibles et leur présentation doit être claire et nette (article 6, paragraphe 1, point 3 de la loi TMG).

Exemple :
Une boutique en ligne XY propose une remise limitée dans le temps. Dans la newsletter, elle en fait de la publicité avec le titre « Super promotion d'été chez XY - maintenant, 20% de remise sur tous les articles déjà réduits ».

Dans un tel cas de figure, le client doit être informé des conditions dans lesquelles il peut prétendre à la remise, sa date d'expiration et un éventuel minimum de commande. Le client doit également être informé de l'exclusion de certaines marques ou d'articles. De manière idéale, ces informations doivent être fournies à la fin du courriel et être liées à l'offre accroche-regard à travers un astérisque. Alternativement, il est également possible de prévoir une possibilité d'accès aux informations complémentaires via un lien clairement visible.

Les informations de l'exemple ci-dessus pourraient se présenter comme suit : *« Valable du 15 au 31/08/2016, ne vaut que pour les articles réduits, valeur de commande minimum 50 €, les marques A & B sont exclues de la promotion. »*

Pour les loteries ou les concours aussi le caractère publicitaire doit être clairement visible et les conditions de participation doivent être facilement accessibles (article 6, paragraphe 1, point 4 de la loi TMG).

En plus, même une newsletter doit répondre à toutes les prescriptions d'autres lois. En effet, une newsletter est un acte commercial, de sorte qu'il y a lieu de prendre en compte notamment les dispositions stipulées aux lois sur la concurrence déloyale (loi UWG).

Selon cette loi, les affirmations publicitaires ne doivent pas induire en erreur (article 5 de la loi UWG) ou influencer le consommateur de manière illicite (article 4bis de la loi UWG). Par ailleurs, la publicité ne doit pas être déguisée comme information voire comme contenu rédactionnel (point 11 de l'annexe à l'article 3, paragraphe 2 de la loi UWG). Lorsque la publicité divulgue un concurrent, il y a lieu de se conformer aux règles en vigueur pour la publicité comparative (article 6 de la loi UWG). Par conséquent, la publicité par courriel doit toujours répondre aux mêmes critères que la publicité distribuée par d'autres voies.

Lorsque la newsletter indique des prix, il faut veiller à répondre aux règlements relatifs à l'arrêté ministériel sur l'étiquetage des prix (Preisauszeichnungsverordnung, PangV). Selon cet arrêté, tout étiquetage des prix pour le consommateur final doit indiquer que la taxe sur la valeur ajoutée est incluse dans le prix. Les éventuels coûts supplémentaires, comme par exemple les frais d'expédition, doivent également être indiqués clairement. De plus, un prix de base doit être indiqué pour certains produits (article 2, PangV).

Lorsque la newsletter utilise des contenus protégés par des droits d'auteur, il y a lieu de veiller à se procurer les droits d'exploitation requis à cet effet. Ceci vaut à la fois pour les photos ou les graphiques comme pour les textes.

Liste de vérification, contenu :

- ✔ le caractère commercial est clairement visible ;
- ✔ pour les promotions à remise, primes ou cadeaux, les conditions sont facilement accessibles et indiquées de manière claire et nette ;
- ✔ pour les loteries et les concours, les conditions de participation sont facilement accessibles et indiquées de manière claire et nette ;
- ✔ les affirmations publicitaires ne sont pas déloyales, p. ex. n'induisent pas en erreur ;
- ✔ les indications des prix répondent aux prescriptions légales, p. ex. la taxe sur la valeur ajoutée, les frais d'expédition, les informations sur les prix de base ;
- ✔ les licences pour les contenus tombant sous des droits d'auteurs ont été obtenues.

4.3 Identification de l'expéditeur

La loi stipule que l'expéditeur de la newsletter doit être clairement identifiable (article 6, paragraphe 1, point 2 de la loi TMG). Ce n'est pas l'expéditeur effectif qui est visé, mais le publicitaire au nom duquel

la newsletter a été envoyée. Il n'est donc pas nécessaire de pouvoir identifier le collaborateur Monsieur X responsable de la newsletter, mais l'entreprise au nom de laquelle Monsieur X a envoyé la newsletter.

Il est illicite de voiler ou de cacher l'expéditeur du courriel (article 6, paragraphe 2 de la loi TMG). Dans l´exposé des motifs, la loi cite l´exemple des informations données sur l'expéditeur suggérant que le courriel proviendrait d'une autorité officielle, p. ex. une administration. Il est également illicite de ne pas indiquer d'expéditeur du tout. Le destinataire doit donc savoir qui a initié l'expédition du courriel.

Lors du choix de l'adresse de l'expéditeur, il y a lieu de veiller à ce que celle-ci donne une impression digne de confiance. Une bonne solution ici serait une adresse clairement identifiable, comme par exemple newsletter@firma.de. Ici aussi, il convient de penser aux filtres à pourriels. Souvent, ceux-ci font automatiquement passer à la trappe les adresses d'expéditeurs douteux.

4.4 Mentions légales juridiquement sûres

Les pages internet doivent comporter des mentions légales. La loi prévoit une obligation de mentions légales pour les pages internet proposées à titre « professionnel » (article 5 de la loi TMG) ainsi que pour les pages internet comportant des contenus à caractère journalistique / rédactionnel (article 55 du traité d'état allemand sur la radiodiffusion, Rundfunkstaatsvertrag, RStV). Par conséquent, toutes les pages internet ne servant pas exclusivement à des fins privées requièrent des mentions légales.

Les mêmes principes s´appliquent également pour les courriels de publicité / newsletters.
Quelles sont les informations obligatoires ?
La loi stipule les informations obligatoires devant figurer au minimum dans les mentions légales :

- nom du fournisseur, pour les sociétés : raison sociale et forme juridique ;
- personnes habilitées à représenter la société (pour les personnes morales) ;
- domiciliation (pas de boîte postale) ;
- adresse courriel ;
- numéro de téléphone et éventuellement de fax ;
- numéro du registre du commerce et des sociétés, registre des coopératives, des associations ou des partenariats, si disponible ;
- le cas échéant : le numéro d'identification intracommunautaire ou numéro d´identification économique ; pour les contenus à caractère journalistique / rédactionnel : indication de l'éditeur (Verantwortlicher im Sinne des Presserechts) ou de la personne responsable du contenu.

Dans certains cas spécifiques, des informations complémentaires peuvent être de mise, p. ex. des informations spécifiques à la profession chez les médecins, les pharmaciens, les avocats ou les conseillers fiscaux.

De plus, il y a également lieu de prendre en compte certaines informations obligatoires relevant du code du commerce et des sociétés. Les informations susceptibles d'être nécessaires sont stipulées au droit commercial et des sociétés allemand. Par exemple, une société anonyme doit publier

des informations différentes qu'un commerçant en nom personnel ou une S.à.r.l de droit allemand (GmbH).

Mentions légales types pour une S.à.r.l de droit allemand (GmbH)

Entreprise type GmbH (S.à.r.l)
représentée par son directeur général Max Durand
1, rue type
12345 Ville type

Courriel : type@type.de
Téléphone : 0123-45 67 89
Fax : 0123-65 43 21
N° d'identification intracommunautaire ou n° d´identification économique: FR 123456789
Tribunal d'instance de type, numéro du registre du commerce 1234

Comment faut-il intégrer les mentions légales ?

Le législateur exige que les informations obligatoires soient

- facilement détectables,
- directement accessibles et
- toujours disponibles.

Par conséquent, les mentions légales doivent également être désignées comme telles et repérables sans recherches astreignantes. La taille des caractères doit être choisie de sorte que le texte soit clairement lisible.

Il n'est pas nécessaire que les informations obligatoires figurent au courriel. Il est également possible d'insérer un lien des mentions légales dans le courriel. La jurisprudence a reconnu que des mentions légales accessibles via 2 clics répondent aux prescriptions légales.

5. Profilage et mesurage du comportement d'ouverture et de clics

L'analyse des intérêts des prospects est possible moyennant l'optimisation du marketing par courriel. On peut affiner le marketing à travers une personnalisation allant jusqu'à l'individualisation. La personnalisation peut être obtenue par une analyse du comportement d'ouverture et de clics des destinataires du courriel, par une analyse d'autres intérêts connus de la personne concernée et de la combinaison des différentes possibilités. La référence juridique pertinente pour la licéité de cette manière de procéder est le droit de la protection des données.

5.1 Application du droit de la protection des données

Il y a lieu de se conformer au droit de la protection des données tant que des données personnelles sont collectées ou exploitées (article 1, paragraphe 2 de la loi BDSG). Sont concernées par ces dispositions toutes les informations relatives à une personne physique spécifique ou identifiable. Ainsi, ce qui compte, c'est de savoir si les données collectées et exploitées peuvent être attribuées à une personne physique spécifique ou identifiable.

Dans le monde professionnel des juristes, les conditions devant être remplies pour un tel caractère identifiable et donc pour l'applicabilité du droit de la protection des données font l'objet de fortes controverses. De manière simplifiée, voici le contenu succinct des discussions : selon l'approche dite subjective, la question décisive est de

savoir si l'organisme détenant les données est lui-même en mesure de faire le lien avec une personne. Cette opinion prévaut notamment dans la littérature juridique et dans la jurisprudence des instances supérieures. L'approche dite objective, en revanche, pose la question de savoir si ceci est toujours impossible même en chargeant éventuellement des tiers externes. Les autorités allemandes chargées de la protection des données ont, elles aussi, tendance à adopter ce dernier avis. La pertinence dans la pratique de ce doute est apparente en raison des interprétations divergentes par la jurisprudence et les autorités de tutelle.[3] Sur le fond, la cour fédérale de justice BGH, elle aussi, tendance à adopter l'approche subjective. La cour a soumis la question à la Cour de Justice de L'Union Européenne (CJUE).[4] En effet, la décision doit être prise sur la base de l'interprétation du droit européen de la protection des données (directive sur la protection des données 95/46/CE). La décision de la CJUE est attendue pour 2016.[5]

Mais il existe un consensus général selon lequel le droit de la protection des données n'est pas applicable aux données anonymes ou bien rendues anonymes. D'après la définition de l'article 3, paragraphe 6 de la loi BDSG, le fait de rendre des données personnelles anonymes consiste en la modification de données personnelles de sorte que les caractéristiques individuelles relatives à la situation personnelle ou de fait ne sauraient plus ou seulement en déployant des moyens irraisonnables de temps, de frais et de ressources humaines être liées à une personne physique spécifique ou identifiable. Il est évident que la question de savoir à quel moment ceci est le cas est également liée à l'interprétation du caractère identifiable d'une personne. Il y a lieu d'en différencier le fait de rendre des données anonymes d'une pseudonymisation. Selon la définition de l'article 3, paragraphe 6 de la loi BDSG, la pseudonymisation consiste à remplacer le nom et d'autres caractéristiques d'identification par un sigle dans le but d'exclure ou de rendre nettement plus difficile l'identification de la personne concernée.

La différence essentielle en est : c'est le droit de la protection des données qui régit la collecte et l'exploitation de données anonymes. C'est le droit de la protection des données qui régit sans aucune restriction la collecte et l'exploitation de données pseudonymisées. Le droit de la protection des données allège toutefois l'exploitation de données pseudonymisées (cf. ci-dessous à l'article 15, paragraphe 3 de la loi TMG).

Le droit de la protection des données régit toutes les activités se rapportant aux données personnelles (cf. article 3, paragraphes 2 à 6 de la loi BDSG). Il n'est donc pas possible de trouver une « issue » du droit de la protection des données via le type de l'activité.

Ce qui est également essentiel, en plus de l'application du droit de la protection des données, c'est de savoir quel droit de la protection des données est applicable : la loi

3 Dans tous les détails et de manière explicite : Eckhardt, dans : Big Data im Marketing, éditeur Dr. Schwarz, Haufe; Eckhardt, CR 2011, 339; Brink/Eckhardt, Editorial, ZD 1/2015 et ZD 2015, 205 et suiv..

4 BGH, décision du 28/10/2014, IV ZR 135/15, CR 2015, 110 et suivants avec annotations Eckhardt (CR 2015, 114 et suiv.)

5 Dans cette affaire C-582/14, l'avocat général a rendu son réquisitoire le 12/05/2016.

fédérale sur la protection des données (BDSG) ou les dispositions relatives à la protection des données stipulés à la loi sur les télémédias (article 11 et suivants de la loi TMG). La délimitation entre la loi BDSG et la loi TMG n'est pas clairement définie par les lois, de sorte qu'il est évident qu'il existe des divergences dans le monde professionnel des juristes. De manière simple, on peut toutefois résumer la délimitation comme suit : les dispositions de la loi TMG sont applicables aux faits spécifiques à l'internet, alors que la loi BDSG s'applique à tous les autres cas (à l'exception du domaine de la télécommunication).[6] Pour le contexte qui nous préoccupe, on présume l'application des articles 11 et suivants de la loi TMG.

5.2 Profils d'exploitation dans le marketing en ligne et par courriel

En ce qui concerne la création de profils d'exploitation en ligne pour le marketing en vertu de l'article 15, paragraphe 3 de la loi TMG, les dispositions relatives à la protection des données de la loi TMG prévoient un règlement spécial :

« Le fournisseur des services est en droit de créer des profils d'exploitation en se servant de pseudonymes aux fins de publicité, de recherche du marché ou de la conception répondant aux besoins, sauf si l'utilisateur s'y oppose. Le fournisseur est tenu à attirer l'attention de l'utilisateur à son droit d'opposition dans le cadre de l'information prévue à l'article 13, paragraphe 1. Ces profils d'utilisation ne doivent pas être réunies avec les données relatives à la personne pseudonymisée. »

6 *Pour plus de détails : Eckhardt, dans : Big Data im Marketing, éditeur Dr. Schwarz, Haufe*

Il en résulte trois options pour le profilage :

- profils personnels : licéité uniquement avec un consentement ;
- profils d'exploitation pseudonymisés : licéité sous les conditions stipulées à l'article 15, paragraphe 3 de la loi TMG ;
- profils d'exploitation rendus anonymes : aucune restriction au niveau du droit de la protection des données, faute d'application du droit de la protection des données (cf. ci-dessus, ch. 5.1).

Théoriquement, l'obtention du consentement offre la marge de manœuvre la plus large pour un profilage. Les prescriptions ci-dessus s'appliquent de la même manière au consentement (cf. chapitre 2). Dans la pratique, ce sont notamment les aspects suivants qui constituent des obstacles pour l'obtention d'un consentement permettant la création de profils en ligne :

(1) avant de commencer la collecte des données, il faut demander à la personne concernée si elle en est d'accord, et ceci de sorte qu'elle y consente clairement, la seule approche « elle doit s'y attendre » ne suffisant pas ;

(2) il faut expliquer de manière compréhensible à la personne concernée ce qui est fait concrètement - donc la manière dont ses données sont exploitées et analysées.

Souvent, le marketing par courriel personnalisé ne permet pas une utilisation de données anonymes. En effet, le but est justement une publicité faite à un destinataire concret, identifié par son adresse courriel devant recevoir le marketing par courriel. C'est au plus tard avec l'affectation à un destinataire identifié que les données jusqu'alors anonymes deviennent des données personnelles.

Selon l'article 15, paragraphe 3 de la loi TMG, la création de profils d'exploitation dits pseudonymisés est licite sous ces trois conditions. Ces trois conditions doivent toutes être remplies.

- **Il faut utiliser des pseudonymes.**

Le terme de la pseudonymisation a déjà été traité au chiffre 5.1 ci-dessus.

- **La personne concernée a été informée de son droit d'opposition à la création de profils d'exploitation dans le contexte de la collecte de ses données; une information a posteriori ne suffit pas.**

Il résulte de l'information sur le droit d'opposition que la personne concernée doit également être informée que des profils d'exploitation seront créés. L'information doit être fournie au début de l'exploitation du service par la personne concernée. Une information après un tel début, voire même après la conclusion du profilage, ne suffit pas.

Il ressort toutefois de la prise de position des autorités allemandes de tutelle de la protection des données relative à Google Analytics[7] qu'une information donnée dans la politique dite Privacy Policy (article 13, paragraphe 1 de la loi TMG) sur le site web suffit.

- **Le profil d'exploitation ne doit pas être réuni avec les données relatives à la personne pseudonymisée.**

Cela signifie que la règle stipulée à l'article 15, paragraphe 3 de la loi TMG n'est applicable que si le profil n'est pas lié à la personne concernée concrète, plus tard non plus.

5.3 Conséquences pour le marketing par courriel

Ces règles, notamment celles stipulées à l'article 15, paragraphe 3 de la loi TMG, s´appliquent à tous les profilages en ligne. Ceci exclut à la fois la collecte et l'analyse du comportement d'ouverture et de clics d'un destinataire de courriels tout comme la collecte de données par tout autre moyen.

Cette disposition offre une possibilité pour l'exploitation de données personnelles. Le maintien de la pseudonymisation lors de l'exploitation du profil représente un défi qui se pose souvent. Il n'existe aucune solution juridique générale à ce problème, mais il y a lieu d'examiner la conception concrète dans chaque cas spécifique.

7 *Décision de l'autorité de tutelle suprême pour la protection des données dans le domaine non public du 26 et 27 novembre 2009 à Stralsund, conception conforme à la protection des données de procédés d'analyses relatifs au mesurage de la portée d'offres faites dans l'internet*

6. Traitement de données par des prestataires de services externes lors du recours à des prestataires de services

En cas de recours à des prestataires de services (externes) pour le marketing par courriel, il y a lieu de remettre en question leur implication du point de vue de la protection des données. Les prestataires de services externes peuvent être des fournisseurs de logiciels (notamment les services de nuage) pour les solutions GRC et d'expédition, des agences, des fournisseurs de contenus, des prestataires d'analyses, etc. Lors du recours à des prestataires de services, il convient également de se conformer aux règles de la protection des données. Ce n'est pas dans tous les cas de recours à des prestataires de services que le droit de la protection des données est pertinent.

Ce qui compte pour l'application du droit des données, c'est de savoir si les prestataires de services ont accès à des données personnelles. La question de savoir quand il y a lieu de présumer l'existence de données personnelles a déjà été expliquée au chiffre 5.1 ci-dessus. Lorsque le prestataire de services doit traiter les données personnelles (p. ex. les préparer, enrichir, comparer), l'application du droit de la protection des données est claire. Or, si son intervention est limitée à une seule possibilité d'accès, se pose alors la question de savoir si cela suffit déjà pour l'application du droit de la protection des données. La délimitation est difficile et il n'existe pas d'appréciation homogène dans le monde des professionnels. Par mesure de sécurité, il conviendrait donc de se poser la question de savoir si le prestataire de services peut effectivement accéder aux données et non pas s'il doit le faire ou y est autorisé, pour déterminer l'existence ou non d'un tel accès.

Selon l'avis des autorités allemandes de tutelle de la protection des données, l'application du droit de la protection des données n'est pas exclue même lorsqu'un service de nuage ne comporte que des données cryptées ou le fournisseur du nuage n'a accès qu'à de telles données cryptées. [8] Cependant, ce point de vue est juridiquement contesté.

6.1 Avantage de la conception du traitement de données par des prestataires de services externes

La conception typique du recours à des prestataires de services externes ayant accès à des données personnelles, c'est le traitement de données par des prestataires de services externes (TDP) en vertu de l'article 11 de la loi BDSG. L'avantage qu'offre le TDP, c'est le fait que le transfert de données à un organisme externe de traitement de données ne requiert ni la conformité aux conditions préalables légales en vigueur pour un transfert de données (par exemple l'article 28 de la loi BDSG), ni un consentement de la part de la personne concernée. Cet effet est qualifié d'effet dit de privilégisation du TDP et trouve sa base juridique dans l'article 3, paragraphe 8, phrase 2 de la loi BDSG.[9]

8 *Orientierungshilfe – Cloud Computing der Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Arbeitsgruppe Internationaler Datenverkehr des Düsseldorfer Kreises, version 2.0, du 09/10/2014, pages 12 et suivantes.*

9 *Pour plus de détails : Eckhardt, DUD 2013, 585 et suivants.; Eckhardt/Kramer, DuD 2014, 147 et suivants.*

La condition préalable pour cette privilégisation est toutefois :

(1) la mise en œuvre stricte des prescriptions stipulées à l'article 11 de la loi BDSG (cf. à ce sujet b) ci-dessous) ;

2) les données restent dans l'Union Européenne (UE) voire dans l'Espace Économique Européen (EEE) (cf. à ce sujet 6.3 ci-après).

6.2 Traitement de données par des prestataires de services externes

Un TDP est caractérisé par 3 éléments :

- activité du prestataire de services soumise à des instructions concernant les données personnelles ;
- contrat écrit comportant les contenus en vertu de l'article 11, paragraphe 2, phrase 2 de la loi BDSG ;
- conviction du donneur d'ordre concernant les mesures techniques et d'organisation prises en vue de la protection des données par le prestataire, avant le début du traitement des données comme après, à des intervalles réguliers.

Il y a soumission aux instructions lorsque le prestataire de services ne dispose pas de marge de manœuvre pour la prise de décision par rapport au traitement de données personnelles. En bref : le prestataire de services doit, dans chaque situation qui se présente, savoir ce qu'il doit faire, grâce aux instructions qui lui sont données par le donneur d'ordre. Cette définition se fait typiquement à travers le descriptif des prestations faite dans le contrat ou la commande.

Le contrat portant sur le TDP requiert, selon le droit allemand, la forme écrite au sens de l'article 126 du BGB, de sorte qu'une conclusion électronique est exclue, sauf si le contrat est conclu moyennant des signatures électroniques qualifiées en vertu de l'article 126bis du BGB. L'article 11, paragraphe 2, phrase 2 de la loi BDSG prévoit comme contenu minimum de la convention ce qui suit :

1. « L'objet et la durée du contrat ;
2. le volume, le type et le but de la collecte, du traitement ou de l'exploitation prévus de données, le type des données et le groupe des personnes concernées ;
3. les mesures techniques et d'organisation à prendre en vertu de l'article 9 ;
4. la rectification, la suppression et le verrouillage de données ;
5. les obligations du prestataire de services découlant de l'article 4, notamment les contrôles à réaliser par ce dernier ;
6. l'éventuelle habilitation lui permettant de conclure des sous-contrats de prestations ;
7. les droits de contrôle du donneur d'ordre et les obligations y afférentes de tolérance et de collaboration du prestataire de services ;
8. les violations commises par le prestataire de services ou des personnes employées par lui des prescriptions de protection de données personnelles ou des dispositions stipulées à la commande et soumises à l'obligation d'informer ;
9. l'envergure du pouvoir de direction que le donneur d'ordre se réserve vis-à-vis du prestataire de services ;
10. la restitution de supports de données remises et la suppression de données stockées chez le prestataire de services à la fin du contrat ».

La conviction du donneur d'ordre par rapport aux mesures techniques et d'organisation pour la protection des données par le prestataire de services ne doit pas obligatoirement se faire sur place chez ce dernier et par le donneur d'ordre lui-même. Il y a des controverses au sein des milieux professionnels quant à l'envergure dans laquelle le donneur d'ordre est en droit de se fier aux affirmations faites par le prestataire de services. Les certificats, labels de qualité et audits par les tiers indépendants et techniquement compétents englobant l'intégralité de l'éventail de la commande, sont une solution préférable.[10]

6.3 Traitement de données transfrontalier par des prestataires de services externes

Lorsque les données personnelles sont transférées de manière transfrontalière respectivement lorsque l'on y accède à partir d'autres pays (cf. introduction au chiffre 6), une vérification complémentaire (!) de la licéité d'un tel transfert de données est nécessaire au niveau du droit de la protection des données pour être licite (article 4ter, 4quater de la BDGS).

L'appréciation peut tout simplement être divisée en deux parties : lorsque les données voire l'accès restent au sein de l'UE ou bien de l'EEE, il n'existe aucune contrainte supplémentaire quant à la licéité. Lorsque les données sont transférées ou si l'accès se fait en dehors de l'EU ou de l'EEE, les dispositions des lettres b) et c) de l´article 4 de la loi BDSG stipulent une vérification pour savoir s'il existe un niveau de protection des données adéquat pour le destinataire dans son pays.[11] Le fait que l'effet dit de privilégisation du TDP est supprimé en vertu de l'article 3, paragraphe 8, phrase 2 de la loi BDSG (cf. ci-dessus) complique davantage la situation. Il faudrait donc examiner aussi la question de savoir s'il existe ou non une règle de licéité légale pour le transfert ou bien l'accès.[12] En fin de compte, c'est un examen à deux niveaux qui est de mise : 1° licéité du transfert voire de l'accès en vertu de l'article 28 ou de l'article 29 de la loi BDSG ; 2°. licéité du transfert dans le pays concerné en vertu des articles 4ter, 4quater de la BSDG.

6.4 La responsabilité du donneur d'ordre

Le donneur d'ordre du prestataire de services doit être conscient de sa responsabilité sous deux aspects :

le transfert de données au prestataire de services - même si celles-ci sont transférées à l'étranger - ne le dégage pas des restrictions imposées par le droit allemand en matière de la protection des données quant au maniement de ces données. En quelques mots : ce qui est interdit au donneur d'ordre sur ses propres systèmes lui est également interdit sur les systèmes du prestataire de services. La responsabilité du donneur d'ordre vis-à-vis de ceux dont les données sont traitées reste entièrement

10 *Pour plus de détails : Leitfaden – Datenschutz und Cloud Computing, Leitfaden Nr. 11, Kompetenzzentrum Trusted Cloud, pages 19 et suivantes.*

11 *Ici, en plus de détails : EuroCloud Leitfaden Recht, Datenschutz & Compliance, http://www.eurocloud.de/2010/news/datensicherheit/eurocloud-leitfaden-recht-datenschutz-compliance.html; Leitfaden – Datenschutz und Cloud Computung, Leitfaden Nr. 11, Kompetenzzentrum Trusted Cloud, pages 27 et suivantes.*

12 *Dans le cas typique, le consentement de toutes les personnes concernées est à écarter comme option de conception.*

engagée en vertu de l'article 11, paragraphe 1 de la loi BDSG. Des dommages-intérêts pourraient être revendiqués pour les erreurs commises par ses prestataires de services (article 278 du BGB).

La responsabilité du donneur d'ordre est également engagée pour la conception en bonne et due forme de la convention relative au TDP. Ceci résulte de l'article 11 de la loi BDSG. Cette responsabilité se concrétise par les amendes prévues à l'article 43, paragraphe 1, point 2, lettre b) de la loi BDSG, dirigées exclusivement contre le donneur d'ordre. En revanche, le prestataire de services peut se voir infliger des amendes même en cas d'un TDP invalide, notamment en vertu de l'article 43, paragraphe 2, point 1 de la loi BDSG ou en tant que partie impliquée dans des infractions commises par le donneur d'ordre. Si le prestataire de services a rédigé le contrat via le TDP, ceci pourrait justifier un droit aux dommages-intérêts de la part du donneur d'ordre. Bref : la bonne conception du TDP est dans l'intérêt des deux parties.[13]

7. Règlement général de l'UE sur la protection des données – un pronostic

Le règlement général de l'UE sur à la protection des données a été publié le 04/05/2016 au Journal Officiel de l'Union Européenne[14], est entré en vigueur le 25/05/2016 et sera applicable conformément à son article 99 à compter du 25/05/2018. De ce fait, le processus législatif entamé le 25/01/2012 sera terminé.[15] Le règlement général règle la protection des données de manière exhaustive.[16]

L'application d'un règlement de l'UE est prioritaire par rapport à tout droit national en conflit. Les règlements dérogeants nationaux sont possibles uniquement dans la mesure où le règlement général prévoit des clauses d'ouverture y afférentes.[17] En quelques mots : le règlement général annule et remplace le droit national de la protection des données et ne prévoit des exceptions que dans certains domaines bien précis.

13 *L'autorité régionale bavaroise de tutelle pour la protection des données (BayLDA), par exemple, a fixé une amende s'élevant à plusieurs dizaines de milliers d'euros dans le cas d'une passation de commande insuffisante (communiqué de presse de la BayLDA « Auftragsdatenverarbeitung ohne richtigen Vertrag kann teuer werden » 20/08/2015).*

14 *Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), JO L 119 du 4/5/2016.*

15 *Pour le contexte : Eckhardt CR 2012, 195 et suivants sur le projet de l'époque élaboré par la commission européenne.*

16 *De manière explicite et pour plus de détails : Eckhardt/Kramer, Datenschutz Aktuell – Spezialreport EU-Datenschutz-Grundverordnung, TKMmed!a*

17 *De manière explicite et pour plus de détails : Eckhardt/Kramer, Datenschutz Aktuell – Spezialreport EU-Datenschutz-Grundverordnung, TKMmed!a*

À l'instar des lois nationales, les dispositions stipulées au règlement général requièrent une interprétation et ne sont pas toujours claires et cohérentes à tous les points de vue. C'est justement en raison du processus législatif européen qu'il subsiste des questions devant toujours être élucidées.[18]

Ci-après, nous fournissons une première vue d'ensemble des répercussions auxquelles il faut s'attendre pour le marketing par courriel.

7.1 Validité des consentements limitée au-delà du 25/05/2018 ?

Le considérant 171 du règlement général prévoit, pour l'essentiel, que tout traitement de données personnelles doit se conformer au règlement général d'ici le 25/05/2018.[19] Il n'y a aucune protection au-delà du 25/05/2018. Ce règlement prévoit les clauses suivantes pour le consentement :

« ... Lorsque le traitement repose sur un consentement donné en vertu du règlement 95/46/CE, il n'est pas nécessaire que la personne concernée y consente de nouveau lorsque le type du consentement déjà fourni remplit les conditions dudit règlement de sorte que le responsable puisse poursuivre le traitement après la date d'entrée en vigueur du présent règlement. »

De ce fait, un consentement continue à être en vigueur lorsque deux conditions préalables ont été remplies :

(1) le consentement répond aux exigences de la directive 95/46/CE ; ce sont des contraintes que la cour fédérale de justice BGH a déjà traitées dans sa décision « Einwilligung in Werbeanrufe II » [20] (consentement aux appels publicitaires) et qui « se reflètent » désormais dans l'article 4, point 11 du règlement général ;

(2) les « conditions » du règlement général ont été remplies. Selon son libellé, il s'agit uniquement des contraintes stipulées aux articles 7, 8 du règlement général. Dans ce cas, les exigences quant à la transparence prévues aux articles 13, 14 ne constitueraient pas de conditions préalables à la validité.

7.2 Règlement du consentement

Le règlement du consentement comporte plusieurs parties dans le règlement général. L'article 4, point 11 du règlement général définit la notion du consentement et détermine les exigences de base. Ceci n'est pas entièrement nouveau à l'interprétation qui a été faite du terme à ce jour, ceci notamment suite à la décision « Einwilligung in Werbeanrufe »[21] de la cour fédérale.

L'article 7 du règlement général stipule des « conditions » complémentaires au consentement. Les principes imposés ne sont pas intégralement nouveaux, mais pour ce qui est des détails, il faudra toutefois

18 *De manière explicite et pour plus de détails : Eckhardt/Kramer, Datenschutz Aktuell – Spezialreport EU-Datenschutz-Grundverordnung, TKMmed!a*

19 *De manière explicite et pour plus de détails : Eckhardt/Kramer, Datenschutz Aktuell – Spezialreport EU-Datenschutz-Grundverordnung, TKMmed!a*

20 *BGH, décision du 25/10/2012, I ZR 169/10, MMR 2013, 380 et suivants avec annotations Eckhardt (p. 382 et suiv.).*

21 *BGH, décision du 25/10/2012, I ZR 169/10, MMR 2013, 380 et suivants avec annotations Eckhardt (p. 382 et suiv.).*

apprécier de quelle manière ceux-ci entraîneront des modifications au niveau de la situation de droit actuelle. Ce qui est nouveau, c'est l'obligation généralisée d'informer la personne concernée de son droit à révoquer son consentement, ceci avant même qu'elle ne le donne (article 7, paragraphe 3, phrase 3 du règlement général). C'est notamment pour les consentements à la réception de publicité que ceci a typiquement déjà été mis en œuvre en raison de l'article 28, paragraphe 4, phrase 2 de la loi BDSG, article 7, paragraphe 4, lettre c) de la loi UWG ainsi que, pour les consentements électroniques, en raison de l'article 13, paragraphe 3 de la loi TMG.

L'article 8 du règlement général comporte des « conditions pour le consentement donné par un enfant en relation avec les services de la société d'informations ». Il y a lieu de s'y conformer dans tous les cas de figure quand il s'agit d'enfants. Il y a lieu d'élucider à l'avenir si des mesures seront nécessaires pour les consentements en général.

Dans la pratique, ceci signifie qu'il convient d'examiner si et le cas échéant quels déficits existent entre les consentements déjà en place par rapport aux exigences prévues au règlement général. C'est à partir de cette base qu'il faudra apprécier si et quand une demande de consentement doit être ajustée et si des mises à jour sont nécessaires pour les consentements déjà obtenus.

7.3 Règles de transparence

Les articles 13, 14 du règlement général prévoient des obligations d'information générales à satisfaire de manière proactive. Les règles s'appliquent différemment aux questions de légalité et au consentement. L'article 13 du règlement général est applicable dans le cas d'une collecte de données personnelles auprès des personnes concernées et l'article 14 du règlement général s'applique lorsque les données personnelles ne sont pas collectées auprès de la personne concernée.

Les obligations d'information sont élargies de manière significative par rapport aux obligations stipulées aux lois sur la protection des données déjà en place. Ici, il y a lieu de procéder à des ajustements dans tous les cas de figure.

L'article 21 du règlement général comporte sa propre règle quant au droit de révocation de la personne concernée. Ceci ne vaut toutefois pas pour le consentement.

Même si la violation de l'obligation d'information ne devait pas entraîner l'invalidité du consentement, la sanction de la violation s'élèvera à une amende pouvant atteindre 20 millions d'euros ou 4% du chiffre d'affaire annuel réalisé dans le monde entier pour l'exercice précédent, le chiffre le plus élevé faisant fois (article 83, paragraphe 5 du règlement général).

7.4 Profilage

Pour le marketing, aucune règle spéciale n'est prévue pour le profilage qui soit comparable à celles stipulées à l'article 15, paragraphe 3 de la loi TMG. L'article 22 du règlement général traite du profilage dans la mesure où ceci fait partie d'une décision automatisée déployant un effet juridique vis-à-vis de la personne concernée ou l'affectant de manière similaire. Dans les cas typiques, ceci

ne sera pas le cas dans le profilage aux fins de marketing, mais il convient de l'examiner au cas par cas.

Dans le cadre du règlement général, ce sera l'intérêt général stipulé à l'article 6, paragraphe 1, lettre f) du règlement général qui sera envisageable comme base juridique pour un profilage aux fins de marketing. Selon ce règlement, il y a lieu de procéder à une pondération des intérêts. Dans la mesure où les données personnelles doivent être exploitées suite à un changement du but pour le profilage aux fins de marketing, il y a également lieu d'intégrer dans l'examen l'article 6, paragraphe 4 du règlement général.

Pour un tel profilage, il y a lieu de se conformer aux règles de transparence prévues aux articles 13, 14 du règlement général (cf. ci-dessus) et notamment aussi à la règle relative au droit de révocation stipulée à l'article 21 dudit règlement (cf. ci-dessus). La question de savoir si une violation des règles de transparence entraîne l'illégalité du traitement fera certainement l'objet de discussions. Pour les constellations de la loi BDSG en place à ce jour, il y a été répondu par la négative ; mais ceci n'est pas la seule référence pour une interprétation du règlement général conforme à l'UE.

7.5 Traitement par des prestataires de services externes

Le traitement par des prestataires de services externes (tel qu´il est appelé au règlement général) est réglé à l'article 26 du règlement général. L'effet de privilégisation est également stipulé à l'article 4, point 10 du règlement général étant donné que le prestataire de services externe n'est pas considéré comme un tiers. Mais la discussion de savoir si ceci est suffisant pour l'effet de privilégisation a déjà commencé.

La conception du contenu du traitement par des prestataires de services externes est comparable à celle prévue à l'article 11 du règlement général, même s'il y a, bien entendu, des différences et les répercussions de celles-ci doivent être examinés dans le détail.

Ce qui est nouveau, en revanche, c'est qu'en vertu de l'article 82 du règlement général, le prestataire de services externe sera, en principe, solidairement responsable avec le donneur d'ordre (article 82, paragraphe 4 du règlement général). Mais pour le prestataire de services externe, il y a des possibilités de restrictions. Ici, le prestataire de services sera obligé de prendre les mesures nécessaires.

Ce qui est nouveau du point de vue allemand, c'est le terme dit « joined controllership », prévu à l'article 26 - en clair : parties solidairement responsables du traitement. Se posera alors la question de savoir dans quelle mesure le prestataire sera solidairement responsable avec le donneur d'ordre à l'exclusion, désormais, du rapport donneur d'ordre - prestataire de services externe. La condition préalable en vertu de l'article 26, paragraphe 1, 1ère phrase du règlement général, c'est que les buts et les moyens du traitement soient déterminés ensemble. Dans la pratique se posera alors la question de savoir quel rapprochement sera nécessaire. Ici aussi, le prestataire de services sera obligé de prendre les mesures nécessaires.

7.6 Directive ePrivacy (directive 2002/58/CE)

Conformément à son article 95, le règlement général n'impose aux personnes physiques ou morales aucune obligation supplémentaire par rapport au traitement dans le contexte d'une mise à disposition de services de communication électroniques accessibles au public dans des réseaux de communication publics dans l'Union Européenne, dans la mesure où ces personnes sont soumises notamment aux obligations stipulées à la directive 2002/58/CE poursuivant le même but.

Pour simplifier : dans le cadre de la directive 2002/58/CE, le législateur national peut toujours édicter des règles. En Allemagne, cette directive a été transposée dans les dispositions relatives à la protection des données stipulées à la loi allemande sur les télécommunications (article 91 et suivants de la loi TKG). Toutefois, la loi TKG ne règle non seulement des exigences issues de ladite directive, la définition du domaine d'application elle aussi diverge de celle de l'article 95 du règlement général. Ici, des mesures devront être prises par le législateur national afin d'élucider cette question.

Ce qui est plus intéressant dans le contexte qui nous préoccupe, en revanche, c'est la discussion pour savoir si les contraintes imposées par la directive dite directive de témoins de connexion - qui est en fin de compte une directive en modification de la directive 2002/58/CE - a, oui ou non, déjà été intégrée dans les dispositions de la protection des données stipulées à la loi TMG. De ce fait, il est possible que des dispositions de la protection des données stipulées à la loi TMG puissent perdurer même sous le règlement général. Par ailleurs, les dispositions de la protection des données stipulées à la loi TMG (article 11 et suiv. de la loi TMG) seront « annulées et remplacées ». Ici, des mesures devront être prises par le législateur national afin d'élucider cette question.

7.7 Conclusions

Le règlement général de l'UE implique la nécessité de modifications et d'ajustements qu'il y a lieu de réaliser d'ici le 25/05/2018. Ceux-ci doivent toutefois être précédés d'une analyse approfondie de la situation. Cette analyse doit notamment englober la clarification de questions relatives à l'interprétation et à l'application du règlement général. En quelques mots : une agitation stérile est tout aussi inutile que de « rester les bras croisés ».

8. Points à respecter pour le marketing par courriel dans les autres pays

8.1 Les aspects juridiques en Suisse

Alors que l'envoi de courriels de publicité est soumis à une réglementation stricte dans l'UE et spécifiquement en Allemagne depuis un certain temps déjà, le législateur suisse a créé des bases juridiques en 2007 seulement. Cette réglementation se trouve d'une part dans une loi sur la concurrence déloyale (Gesetz gegen den unlauteren Wettbewerb, UWG, article 3, lettre o)) et d'autre part dans une loi sur les télécommunications (Fernmeldegesetz, FMG, article 45, lettre a). L'UWG règle essentiellement les conditions applicables à l'envoi de courriels à caractère commercial. La loi FMG détermine les mesures que le fournisseur de services de télécommunications doit prendre contre les pourriels.

L'état lui-même (le secrétaire d'état pour l'économie, SECO, www.seco.admin.ch) peut prendre des mesures contre les expéditeurs de pourriels sur le territoire national comme à l'étranger lorsqu'un nombre suffisant de personnes se plaint.

Après la révision de la loi suisse sur la protection des données (Datenschutzgesetz, DSG) 2006 - les dispositions y afférentes sont entrées en vigueur en 2008 - même le droit de la protection des données a perdu de sa pertinence en ce qui concerne le marketing par courriel. Ceci d'une part lorsque l'article 3, lettre o) de la loi UWG concernant les courriels de publicité n'est pas applicable parce qu'il ne s'agit pas de publicité de masse automatisée, mais d'autre part aussi en complément à l'article 3, lettre o) de la loi UWG en cas de publicité de masse.

Dans le contexte du marketing par courriel, ce sont les paragraphes 3 et 4 de l'article 4 de la loi DSG qui sont pertinents. L'article 4, paragraphe 3 de la loi DSG stipule l'obligation dite d'affectation. Les données personnelles ne doivent être traitées qu'aux seul but indiqué lors de l'obtention des données ou détectable à travers les conditions de collecte. L'article 4, paragraphe 4 de la loi DSG stipule l'obligation dite de transparence. La collecte et le traitement de données personnelles ainsi que le but du traitement doivent être reconnaissables pour la personne concernée. Faute de respecter ces deux principes de traitement des données, ceci constitue une atteinte à la personnalité. Dans un tel cas, l'article 13 de la loi DSG exige une justification (p. ex. le consentement de la personne concernée ou un intérêt supérieur de la personne traitant les données). En cas de violation des principes du traitement des données dans le cadre du marketing par courriel, un consentement est toujours indispensable.

Cette vue d'ensemble des dispositions légales pertinentes pour le marketing par courriel démontre que les exigences légales en Suisse sont beaucoup moins détaillées que par exemple en Allemagne. Il y a beaucoup plus de liberté d'interprétation. Qu'est-ce qui est alors réellement licite et qu'est-ce qui ne l'est pas ?

L'envoi de courriels de publicité à des prospects

« L'envoi en masse de publicité par internet ou des services de télécommunication » à des prospects est juridiquement licite si les prérequis suivants sont remplis :

- le destinataire y a expressément consenti avant la réception des courriels (principe de l'opt-in) (cf. aussi « méthodes d'inscription ») ;
- l'expéditeur est clairement identifiable. Son adresse est indiquée correctement, son identité n'est ni dissimulée, ni falsifiée ;
- chaque courriel de publicité comporte une possibilité clairement visible, gratuite et simple de désabonnement (p. ex. le lien de désabonnement muni d'une confirmation de suppression, éventuellement même un lien conduisant vers un formulaire de suppression).

Un consentement est également nécessaire du point de vue du droit de la protection des données. Pour les courriels de publicité adressés aux prospects, le principe de transparence prévu par le droit de la protection des données n'est régulièrement pas respecté.

L'envoi de courriels de publicité à des clients existants

Pour l'expédition de courriels de publicité à des clients existants, l'article 3, lettre o) de la loi UWG prévoit certains allègements. Un destinataire est considéré comme « client existant » lorsqu'il existe déjà un rapport économique entre lui et l'entreprise faisant la publicité, c'est-à-dire qu'un achat doit effectivement avoir eu lieu (prestation de services ou livraison de produits). Pour l'envoi de courriels de publicité à de tels clients existants, aucun opt-in n'est nécessaire, à condition de satisfaire aux prérequis suivants :
il existe un lien entre la prestation fournie au préalable et la prestation objet de la publicité (publicité pour les produits et les prestations de services comparables) ;
il n'y a aucune publicité pour les services externes ; pour l'envoi de courriels de publicité aux clients existants aussi, l'expéditeur doit clairement être identifiable et chaque courriel doit comporter une possibilité de désabonnement gratuite et facilement détectable (cf. ci-dessus).

Faute de satisfaire aux prérequis ci-dessus - par exemple lorsque l'on souhaite envoyer au client existant des informations sur les produits de tiers - il y a lieu de répondre aux mêmes exigences que pour l'envoi de courriels de publicité destinés aux prospects.

Méthodes d'inscription

Le législateur suisse a omis de régler la forme et la démontrabilité de l'inscription dans l'article 3, lettre o) de la loi UWG. L'expéditeur est alors en principe libre dans son choix des méthodes d'inscription indiquées ci-dessus. La seule condition préalable obligatoire est celle d'un consentement « exprès » fourni par le destinataire.

La collecte d'inscriptions hors ligne (p. ex. à l'occasion de salons, par téléphone ou via des formulaires d'inscription physiques dans la boutique de vente) n'est pas non plus soumise à des prescriptions réglant dans le détail la démontrabilité et l'obligation de conservation. Mais en fin de compte, c'est

l'expéditeur qui doit s'assurer que le destinataire ait expressément consenti à la réception de la publicité par courriel.

Il existe les méthodes d'inscription en ligne suivantes permettant de répondre au principe opt-in :

› Single Opt-In
L'abonné s'inscrit en ligne expressément en cliquant sur une case à cocher correspondante ainsi que par la fourniture de son adresse courriel (et éventuellement d'autres données). Son inscription lui est confirmée uniquement sur une page suivante de la page d'inscription. Nous déconseillons vivement cette méthode d'inscription.

› Confirmed Opt-In
L'abonné s'inscrit en ligne expressément en cliquant sur une case à cocher correspondante ainsi que par la fourniture de son adresse courriel (et éventuellement d'autres données). Son inscription lui est confirmée d'une part sur la page suivante et d'autre part par courriel.

Du point de vue de la loyauté, un confirmed opt-in (single opt-in accompagné d'une confirmation par courriel sans lien de confirmation) est licite, mais comporte des risques au niveau du droit de la protection des données. Comme expliqué ci-dessous (cf. double opt-in), l'entreprise traitant des données personnelles doit s'assurer de leur exactitude et veiller à ce que le destinataire ait consenti à la réception de publicité par courriel. Le confirmed opt-in présente certains risques d'abus. On ne saurait exclure p. ex. le risque d'inscription d'une adresse courriel d'autrui par un tiers qui commanderait ainsi une newsletter pour une adresse courriel qui ne lui appartient pas. De ce fait, une entreprise recourant au confirmed opt-in n'aurait aucune possibilité de vérifier si cette inscription a effectivement été fait par le titulaire de l'adresse courriel.

› Double Opt-In:
Dans la pratique, c'est la procédure dite « procédure double opt-in » qui s'est imposée, notamment en vue de la loi sur la protection des données.

Il s'agit d'une procédure durant laquelle un client donne son consentement « en double » (en deux étapes). Dans une première étape, un destinataire indique son adresse courriel, par exemple afin de recevoir une newsletter (1ère étape). Ensuite, l'entreprise faisant la publicité envoie un courriel de confirmation comportant un lien de confirmation à l'adresse indiquée par le destinataire et le destinataire confirme via ce lien de confirmation (par un clic) souhaiter recevoir une newsletter (2e étape).

Même si, du point de vue de la loyauté, un consentement a déjà été donné à la première étape, nous recommandons la manière de procéder du double opti-in en raison du droit de la protection des données. L'expéditeur doit s'assurer de ce que le destinataire ait effectivement consenti à la réception de la publicité. À notre avis, ceci ne saurait être garanti que par la seule procédure double opt-in.

Fonctions « Tell-a-Friend »

En Suisse, les fonctions dites « Tell-a-Friend » sont courantes et largement reconnues comme étant licites, tout au moins les

messages envoyés à l'aide de cette fonction ne sauraient être qualifiés de publicité de masse au sens de l'article 3, lettre o) de la loi UWG. Selon l'exposé des motifs, la publicité de masse représente des messages envoyés de manière automatisée. Les messages publicitaires nécessitant l'intervention humaine - pour la fonction « Tell-a-Friend », c'est la saisie d'adresses de courriel individuelles - ne sont pas considérés comme publicité de masse.

Adresses achetées

Une des questions posées régulièrement est celle-ci : *« Est-il licite d'envoyer des courriels à des adresses achetées / louées ? »*

Selon le droit suisse, nombreuses sont les entreprises faisant de la publicité à évoluer dans des zones grises. Beaucoup d'entreprises faisant de la publicité partent du principe qu'elles peuvent envoyer des courriels de publicité sans aucun problème à des adresses achetées. Ceci n'est pas exact.

La difficulté particulière de l'envoi de courriels de publicité à des adresses achetées consiste en le fait que le publicitaire ne se procure les données pas directement chez la personne concernée. Sans une information adéquate, la personne concernée ne peut savoir que l'adresse courriel procurée est vendue à des tiers à des fins publicitaires. Sans information, ceci constituerait une violation de l'article 4, paragraphe 4 de la loi DSG que l'on ne saurait justifier régulièrement qu'à l'aide d'un consentement (article 13 de la loi DSG). De toutes les manières, un consentement est requis par l'article 3, lettre o) de la loi UWG. Dans le cas idéal, le consentement éclairé doit être assuré par le pourvoyeur des données au moment de l'obtention des données.

L'étendue des informations nécessaires dans le cadre du consentement ne découle de manière suffisamment claire, comme déjà évoqué, ni de l'article 3, lettre o) de la loi UWG, ni de la loi sur la protection des données. Mais les clients voire les personnes concernées doivent être en mesure de se faire une idée sur le groupe des destinataires des données. Lorsque le pourvoyeur des données personnelles souhaite transmettre les adresses à un groupe de destinataires sans restrictions, les exigences quant au consentement sont assez strictes. L'information et le consentement doivent être clairs et nets. Si l'information et le consentement doivent être fournis dans des CGV, le groupe des tiers ne doit pas être trop large, ni d'une composition trop hétéroclite. Une transmission d'adresses moyennant le consentement et l'information dans les CGV devrait par conséquent être licite, par exemple lors d'une transmission à d'autres sociétés d'un groupe, à l'exclusion toutefois d'un nombre illimité de tiers.

Ce qui importe en plus, en vue de l'article 3, lettre o) de la loi UWG, c'est que le publicitaire ne peut se fier à l'assurance donnée par des tiers selon laquelle un consentement suffisant aurait été donné.

Collecte à partir de sources accessibles au public

Beaucoup d'entreprises faisant de la publicité partent du principe qu'il n'y a aucune restriction pour l'exploitation d'adresses courriel collectées à partir de sources publiques. Cet avis souvent entendu est erroné.

Les adresses courriels peuvent être collectées notamment en faisant des recherches dans l'internet. En l'espèce, l'expéditeur de courriels de publicité ne pourra se réclamer ni d'un consentement (implicite ou explicite), ni de relations d'affaires existantes. De ce fait, un envoi licite de publicité par courriel (en conformité avec l'article 3, paragraphe 1, lettre o) de la loi UWG) n'est pas possible.

Même du point de vue de la protection des données, l'exploitation d'adresses courriels collectées à partir de sources publiques pour envoyer des courriels publicité pose problème. La collecte des adresses à partir de sources publiques n'est régulièrement pas reconnaissable pour la personne concernée, par conséquent, il y a violation de l'article 4, paragraphe 4 de la loi DSG. À première vue, le droit de la protection des données semble permettre l'option de se réclamer du fait que les personnes concernées avaient rendu accessibles au public les adresses courriels et que par conséquent l'envoi de courriels de publicité ne constituerait raisonnablement (selon l'article 12, paragraphe 3 de la loi DSG) pas d'atteinte à la personnalité. Or, cette présomption ne vaut que pour le traitement de données dans le cadre du but de publication poursuivi par la personne concernée et dont elle peut s'attendre au vu des circonstances. Une personne publiant son adresse courriel sur son site web ne veut pas forcément inviter à l'envoi de publicité de masse.

Mais le contexte de la publication de l'adresse peut également conduire à ce que le but de la publication couvre l'envoi de publicité ciblé, par exemple l'inscription de l'adresse courriel dans des pages jaunes, des registres, etc.

Attention : principe du lieu du marché

Comme déjà évoqué, la législation suisse est moins détaillée que celle en Allemagne. C'est pourquoi il est compréhensible que la plupart des entreprises suisses ne se conforment pas aux prescriptions détaillées étrangères.

Or, il existe un « pépin » qui n'est pas tout à fait anodin et dont les entreprises suisses devraient être conscients : en effet, lorsqu'une entreprise suisse envoie des courriels à des destinataires à l'étranger, le principe du « lieu du marché » stipule que cet envoi de courriels de publicité doit toujours respecter le droit étranger y afférent (qui est souvent plus détaillé).

Que signifie le terme « principe du lieu du marché » ?

Le lieu du marché est le lieu où l'on cherche à influer sur le destinataire par les moyens du marketing. Les indices permettant de déterminer le lieu du marché sont :

- l'identification de l'adresse courriel (p. ex. @courrielexample.fr) ;
- la langue du courriel ;
- le rapport du produit objet de la publicité fait au pays (p. ex. sites internet allemands).

Si l'on applique la définition ci-dessus de manière stricte, il faut donc présumer pour les abonnés d'une newsletter rédigée en langue allemande que ceux-ci puissent également se situer en Allemagne. De ce fait, le champ obligatoire pour l'inscription doit comporter uniquement l'adresse courriel. En complément, l'entreprise est tenue à pouvoir justifier de manière crédible et sans lacune

une telle inscription - que celle-ci se soit faite hors ligne ou en ligne.

Bien entendu, des facteurs comme la taille de l'entreprise faisant de la publicité ainsi que la question de savoir si l'entreprise travaille au niveau régional, national ou bien même international, jouent un rôle important quand il s'agit de l'importance de cette disposition. Ainsi, on peut présumer que les clients allemands d'une petite entreprise travaillant au niveau local ne s'inscrivent que dans les cas les plus rares pour une newsletter, pour ensuite « oublier » cette inscription et se plaindre par la suite de la réception de courriels non sollicités.

Or, toute entreprise souhaitant profiter des avantages du médium qu'est le courriel afin de prospecter et fidéliser des clients ferait mieux de bien réfléchir si elle souhaite se contenter de respecter « tout juste » les seules contraintes légales pour sa politique de communication ou si ce n'est pas plutôt l'entente bienveillante avec les clients (potentiels) qui devrait constituer les bases pour la communication.

Sanctions prévues en cas de violation des prescriptions légales

Tout acte de concurrence déloyale prémédité en vertu de l'article 3 de la loi UWG est passible d'une peine d'emprisonnement pouvant atteindre trois ans ou d'une peine pécuniaire (article 23 de la loi UWG). Il n'existe à ce jour toutefois pas d'arrêt exécutoire de la cour fédérale relatif à cet état de fait (article 3, lettre o) de la loi UWG). Il semblerait qu'à ce jour, seul le tribunal cantonal de Lucerne aurait traité cet article dans une décision du 1er juillet 2014 (LGVE, I n° 6, 2014). Un destinataire d'un courriel de publicité avait déposé plainte contre une entreprise ayant fait de la publicité. Le Ministère Public avait classé l'affaire sans suite. Suite à un appel interjeté, le tribunal cantonal a confirmé cette décision. Dans le cadre du jugement, le tribunal cantonal a, entre autres, également dit pour droit qu'aucun double opt-in ne serait exigé par la loi. Le cas soumis au tribunal a pourtant démontré pourquoi cette méthode d'inscription doit être recommandée. Dans le cas cité ci-dessus, le destinataire du courriel de publicité avait affirmé n'avoir fourni ni son adresse courriel, ni donné son consentement. L'entreprise ayant fait la publicité avait dit, elle, que l'adresse courriel aurait été saisie sur son site web concernant la réception de la newsletter.

À quelques exceptions près, aucune sanction pertinente n'est prévue dans le droit en vigueur pour les cas de violation de la loi sur la protection des données. La violation de l'obligation de transparence n'est pas soumise aux sanctions pénales par la loi DSG en vigueur tant qu'il ne s'agit que de données « normales » (article 34 de la loi DSG). Il pourrait tout au plus en être autrement si au moment de la collecte de données personnelles issues de sources externes, on aurait collecté, non seulement des adresses courriel devant être qualifiées de données personnelles « normales », mais également des données dignes d'une protection élevée, créant ainsi par exemple un profil de la personne. Dans ce cas, l'article 14 de la loi DSG prévoit une obligation d'information active. La violation de cette obligation peut être sanctionnée par une amende (article 34, paragraphe 1 de la loi DSG). Par ailleurs, la personne concernée

peut à tout moment intenter une action civile (article 15, paragraphe 1 de la loi DSG). Elle peut demander à ce que toute poursuite du traitement des données soit interdite, ou que les données collectées sur elle soient supprimées.

À l'avenir, les sanctions prévues pour les violations de la protection des données doivent être étendues. Le délégué confédératif à la protection des données doit notamment être compétent pour infliger des amendes élevées en cas de contravention contre ses recommandations visant à remédier aux violations de la protection des données. À l'heure actuelle, le projet de révision n'est que dans la phase de consultation des experts. Aucun avant-projet concret n'a été établi à ce jour. Si la révision devait être intégrée dans la législation et le droit suisse révisé de la protection des données devait, selon toutes les attentes, se modeler sur le règlement général européen de la protection des données, les entreprises faisant de la publicité doivent tenir compte du respect de la loi DSG de manière beaucoup plus stricte que c'est le cas à l'heure actuelle.

Ce n'est non seulement le droit qui compte

Même si l'imposition de la loi suisse luttant contre les pourriels est plutôt une conception théorique que pratique, il convient que toutes les entreprises faisant de la publicité se conforment à ceci : il a été prouvé que les clients (potentiels) se sentant dérangés par des « pourriels » développent très rapidement une aversion contre l'entreprise faisant cette publicité. C'est pourquoi nous conseillons tout à fait aux entreprises suisses de respecter les principes juridiques nettement plus détaillés de l'Allemagne ainsi que la procédure double opt-in afin de garantir que tous les abonnés - qu'ils résident en Suisse ou dans les pays voisins - soient contactés en conformité avec la loi. Certes, il est possible que le groupe des destinataires soit légèrement réduit par l'application de la méthode d'inscription « double opt-in », mais n'englobera, en revanche que les lecteurs s'intéressant réellement à l'offre du fournisseur et réagissant de ce fait en conséquence à ses courriels.
La liste de vérification ci-après montre les conditions qu'une entreprise doit impérativement remplir lors de l'envoi de courriels de marketing en Suisse - et les conditions qu'elle peut avantageusement remplir à titre volontaire. La liste de vérification ne doit pas être considérée comme exhaustive. C'est notamment aux grandes et moyennes entreprises que nous recommandons en plus de recourir à un spécialiste de la communication pour l'élaboration des directives du marketing par courriel.

Liste de vérification

- ✔ adresse exacte et claire de l'expéditeur (la vraie identité)
  › Obligation
- ✔ consentement exprès au préalable ou rapport économique existant avec le destinataire (le destinataire est client)
  › Obligation
- ✔ possibilité simple et bien visible de refus pour les envois futurs (la même voie de communication, pas de frais supplémentaires) ; par exemple lien de désabonnement, désabonnement par courriel de réponse
  › Obligation

- ✔ consentement en ligne : la case à cocher qui représente le consentement pour la réception de courriels de publicité de l'expéditeur nécessite un clic actif de la part du destinataire (à l'exclusion d'une case à cocher déjà marquée)
  › **Obligation**
- ✔ les destinataires désabonnés ne sont plus contactés par courriel
  › **Obligation**
- ✔ courriels aux clients existants : aucun envoi de publicité de tiers sans avoir obtenu au préalable leur consentement exprès
  › **Obligation**
- ✔ aucun courriel de publicité automatisé aux adresses courriels qui ont été collectées de sources publiques
  › **Obligation**
- ✔ lors de l'envoi de courriels de publicités à des adresses achetées, il y a obligatoirement lieu d'obtenir une confirmation écrite de la part du vendeur selon laquelle les personnes concernées ont fourni un consentement valable. Dans le cas idéal, l'entreprise faisant de la publicité doit vérifier le consentement valable par échantillons
  › **Recommandation**
- ✔ courriels aux clients existants : aucune publicité pour ses propres produits sans avoir obtenu au préalable leur consentement exprès
  › **Recommandation**
- ✔ mentions légales complètes comportant une possibilité de prise de contact hors ligne (adresse, numéro de téléphone) et garantie de joignabilité de l'expéditeur
  › **Recommandation**
- ✔ inscription en ligne uniquement via double opt-in (traçabilité !)
  › **Recommandation**
- ✔ les consentements obtenus hors ligne sont enregistrés / stockés (traçabilité !)
  › **Recommandation**
- ✔ aucun envoi de courriels aux clients avec qui on n'avait plus de contact depuis longtemps
  › **Recommandation**

d'autres informations utiles sur le sujet : site web du préposé fédéral à la protection des données et à la transparence (PFPDT) :

› **http://www.edoeb.admin.ch/datenschutz/00683/00803/00816/index.html?lang=de**

› **http://www.edoeb.admin.ch/dokumentation/00612/00660/00687/index.html**

› **www.kommunikationsrecht.ch**

8.2 La situation juridique en Autriche

Dans le droit autrichien, le cadre juridique du marketing par courriel est réparti sur différentes dispositions légales dont certains fragments, tout comme en Allemagne, sont des transpositions de la directive correspondante de l´UE. La mise en œuvre pratique de ces dispositions diverge en partie nettement du droit allemand. La vue d'ensemble ci-après se limite aux prescriptions autrichiennes relatives à l'envoi de courriels non sollicités ainsi qu'aux obligations d'information y afférentes et aux dispositions relatives à la protection des données. Les dispositions spéciales prévues aux lois spécifiques à certains secteurs et branches ne sont pas traitées ici. Il y a des parallèles entre les droits de la protection des données autrichien et allemand, le droit autrichien ne

connaissant toutefois pas de pendant aux dispositions de protection des données dans la loi sur les télémédias allemande.

Introduction

Les obstacles à franchir par l'envoi licite de courriel sont stipulés à l'article 107, paragraphe 2, points 3 et 5 de la loi sur les télécommunications 2003 (Telekommunikationsgesetz, TKG 2003). Sont concernés par ces dispositions les courriels envoyés aux consommateurs (B2C) et aux entreprises (B2B). Des dispositions complémentaires sont prévues à la loi e-commerce (E-Commerce-Gesetz, ECG).

Licéité du marketing par courriel - principe de l'opt-in

Tout comme le droit allemand, le droit autrichien prévoit, en principe, une « procédure opt-in ».

Conformément à l'article 107, paragraphe 2 de la loi TKG 2003, un consentement du destinataire du courriel est nécessaire à l'envoi, lorsque

- l'envoi est fait aux fins de publicité directe ou
- s'il s'adresse à plus de 50 destinataires.

De manière similaire que le font les tribunaux allemands, les tribunaux autrichiens ont une conception large du terme publicité directe de sorte à y englober notamment des newsletters et des courriels d'information. Le destinataire doit être protégé d'une atteinte à sa vie privée par des envois électroniques non sollicités ainsi de frais ou d'autres charges. Selon le tribunal administratif autrichien (Verwaltungsgerichtshof, VwGH) [VwGH, 19/12/2013, 2011/03/0198], les dispositions de la loi TKG 2003 sont également applicables à la publicité électorale, étant donné que celle-ci aussi vise à réaliser un impact tout aussi impopulaire. Ici, la seule saisie d'une adresse courriel dans un registre d'adhérents public en ligne ne suffit pas en tant que consentement.

Lors d'un envoi de courriels à plus de 50 destinataires, les dispositions légales stipulent que même les courriels privés sont sujets à la loi TKG 2003. Même si l'importance est faible dans la pratique, les prescriptions de la loi (p. ex. la possibilité de désabonnement) devraient juridiquement être respectées.

Le consentement requis en vertu de la loi doit être obtenu avant l'envoi des courriels. Il n'y a aucune forme préconisée pour le consentement, ce qui signifie que même un consentement implicite serait toujours valable. La charge de la preuve pour l'existence ou non d'un consentement du destinataire incombe toutefois à l'expéditeur du courriel. Il en résulte que la conception de l'obtention du consentement doit en assurer le caractère démontrable. Ici, le droit autrichien comme le droit allemand présentent des problèmes comparables au niveau de la preuve (cf. à ce sujet le chapitre ci-dessus relatif à la charge de la preuve en droit allemand). La procédure « double opt-in » qui prévoit, suite à l'inscription à une newsletter, l'envoi d'un courriel sans publicité en demandant si l'on souhaite réellement obtenir la newsletter, pourrait constituer la norme courante. La confirmation en réponse sera pertinente. De toutes les manières, il n'existe aucune prescription légale quant à la

nature de la procédure d'inscription. Si la conception de la procédure d'inscription est trop compliquée, ceci risque implicitement de toujours générer moins d'inscriptions en fin de compte.

Afin de déterminer le droit applicable dans chaque cas, le principe du pays destinataire est applicable dans la zone de l'UE. Il y a donc lieu de toujours appliquer le droit auquel est soumis le destinataire du courriel. En Autriche, cette « fiction du lieu du crime » est régie par l'article 107, paragraphe 6 de la loi TKG 2003. À ce sujet, le tribunal administratif VwGH a expliqué [VwGH, 19/12/013, 2012/03/0052] que déjà le principe de protection de la disposition prévoit que le site du serveur n'a aucune importance. Même si l'on ne saurait déterminer l'endroit où le courriel serait finalement appelé, ceci ne serait (selon la VwGH) pas une excuse pour une violation des dispositions légales applicables.

Licéité du marketing par courriel - « opt-out » en tant qu'exception

L'article 107, paragraphe 3 de la loi TKG 2003 prévoit – de manière similaire à l'article 7, paragraphe 3 de la loi UWG allemand - une exception au principe de l'opt-in pour le cas des relations clients existantes. Ceci est dû au fait que les dispositions autrichiennes, à l'instar de celles d'Allemagne, reposent sur une directive européenne.

Conformément à l'article 107, paragraphe 3 de la loi TKG 2003, il existe une exception de la nécessite d'un consentement lorsque

- le destinataire a reçu les coordonnées pour le message dans le contexte d'une vente ou d'une prestation de services à son client, ET
- le message est envoyé pour des produits ou prestations similaires et propres à l'expéditeur, ET
- le destinataire a eu l'occasion claire et nette, lors de la collecte et en complément lors de chaque transfert, de refuser sans problèmes et sans frais une telle exploitation de ses coordonnées électroniques ; ET
- le destinataire n'a pas refusé la réception d'emblée, notamment en s'abstenant de s'inscrire à la liste prévue à l'article 7, paragraphe 2 de la loi ECG.

Les conditions préalables ci-dessus doivent toutes être remplies, sans exception aucune (« ET »). Faute de satisfaire à l'une de ces conditions préalables, l'exception ne s'applique pas et un consentement est nécessaire. Lorsque la dérogation est reconnue, c'est toutefois l'article 7, paragraphe 1 de la loi ECG qui sera applicable : celui-ci stipule que toute communication commerciale doit dans tous les cas de figure être clairement et nettement identifiable en tant que telle lors de sa réception chez le destinataire.

Le refus d'emblée - la dernière condition préalable citée - ne doit pas obligatoirement être prononcé vis-à-vis de l'expéditeur. Le refus peut également être prononcé moyennant une inscription dans la liste indiquée à l'article 7, paragraphe 2 de la loi ECG - la liste dite « liste ECG » (liste Robinson). C'est pourquoi il y a lieu de procéder tout au moins à une vérification au niveau de cette « liste des refus ». Cette liste est gérée par la société « Rundfunk und Telekom Regulierungs-GmbH » (RTR-GmbH) Elle est disponible au format électronique chez la RTR-GmbH pour consultation et vérification. Il existe trois procédures pour

permettre une vérification à l'aide de cette « liste ECG » (version au 04/05/2016: **https://www.rtr.at/de/tk/TKKS_ECGListe**). Toutes les procédures doivent garantir que les noms réels des personnes inscrites ne soient pas divulgués à l'expéditeur potentiel. La grande particularité de la variante autrichienne de cette « liste des refus » est le fait qu'elle est entrée dans le droit et donc imposable dans une envergure nettement plus importante. Certes, elle ne saurait protéger définitivement les personnes inscrites contre les pourriels, non plus, n'empêche qu'elle est plus efficace. Dans beaucoup d'autres pays, les listes Robinson sont gérées par des associations ou des organismes similaires et ne sont obligatoires que pour leurs propres adhérents ou ne stipulent qu'une soumission des publicitaires à titre volontaire. En Autriche, ceci n'est justement pas le cas. Mais étant donné que c'est toujours le principe du consentement préalable qui s'applique - abstraction faite des relations de clients existantes - la « liste ECG » est privée de domaine d'application dans tous les autres cas.

Exigences quant aux contenus

Conformément à l'article 107, paragraphe 5 de la loi TKG 2003, l'identité de l'expéditeur ou du donneur d'ordre de l'envoi du courriel dans le cadre de la publicité directe ne doit être ni dissimulée, ni cachée. Par ailleurs et tout comme en Allemagne, le destinataire doit avoir la possibilité de se désabonner d'une newsletter à tout moment, sans problème et sans frais. Cette possibilité doit être claire et nette, mais ici non plus, il n'existe aucune forme préconisée spécifique. S'il fallait à cet effet procéder en plusieurs étapes, comme par exemple la saisie d'un mot de passe d'un compte d'utilisateur, ceci pourrait, à l'avenir, déjà être considéré par les tribunaux comme étant « trop difficile ». On ne saurait pas non plus déduire de la loi une obligation quelconque pour le destinataire de se conformer impérativement aux contraintes exercées par l'expéditeur. Si l'on se contente de répondre à un courriel, cela devrait suffire comme désabonnement. Or, même l'article 107, paragraphe 5 de la loi TKG 2003 prévoit que tout courriel doit toujours comporter une adresse authentique permettant au destinataire d'adresser une invitation d'arrêter l'envoi de tels messages. Ceci est comparable à l'article 7, paragraphe 2, point 4 de la loi UWG allemande.

Obligations d'information

La loi autrichienne sur les médias (Mediengesetz, MedienG) exige dans son article 24 – ainsi que l'article 5 de la loi ECG, dans la mesure où celle-ci est applicable - l'insertion systématique de mentions légales. Conformément à l´article 1, paragraphe 5, lettre c), la loi MedienG doit être appliquée à la publicité par courriel (médium électronique périodique ou récurrent) dans la mesure où les courriels sont envoyés au moins quatre fois par année calendrier dans une conception comparable. Le domaine d'application de la loi ECG est très large, la simple publication en ligne faite pour des produits suffit pour son application. L'intégration dans le courriel d'un simple lien conduisant aux mentions légales suffit déjà pour répondre à l'obligation de publier des mentions légales, étant donné qu'il n'existe aucune obligation que déjà le message lui-même comporte l'intégralité de ces informations. L'article 25 de la loi MedienG prévoit en plus une divulgation pouvant également être couverte par les mentions

légales. Cette obligation de divulgation est importante en premier lieu pour les personnes morales, étant donné que pour les personnes physiques, elle correspond en principe à la publication des mentions légales prévues à l'article 24 de la loi MedienG. Par conséquent, les indications obligatoires sont fonction de la forme juridique de l'entrepreneur. L'article 25, paragraphe 5 de la loi MedienG prévoit toutefois une exception pour les courriels (newsletter) dont le contenu ne dépasse pas la présentation du domaine de la vie privée et dont le but n'est clairement et en premier lieu pas une influence sur la formation d'opinion publique. Dans un tel cas de figure, l'obligation de divulgation est fortement restreinte et seules quelques informations obligatoires doivent être indiquées. L'article 26 de la loi MedienG inscrit dans la loi l'obligation de clairement marquer comme telles les insertions payantes contenues dans les courriels afin d'éviter d'emblée tout doute quant à leur caractère.

Par ailleurs, les courriels sont également soumis aux dispositions de l'article 14 du code d'entreprises (Untenehmensgesetzbuch, UGB) concernant les « documents d'entreprises et les bons de commande ». La disposition s´applique à toutes les entreprises inscrites au registre du commerce et prévoit des informations différentes en fonction de leur forme juridique. Les informations minimums se recoupent, certes, en majeure partie avec la loi MedienG, mais elles doivent figurer directement dans le message. Pour l'essentiel, il s'agit d'informations juridiques figurant au registre du commerce ainsi que de la structure des sociétés. Un règlement spécial pour les relations d'affaires existantes est prévu à l'article 14, paragraphe 4 u code UGB.

Protection des données

Dès qu'il y a également analyse de données personnelles, il faut se conformer à la loi sur la protection des données 2000 (Datenschutzgesetz, DSG). Pour être en droit d'intervenir au niveau du droit fondamental à la protection des données, certains principes quant à l'exploitation des données doivent être observés. Il s'agit alors notamment du fait que les données sont utilisées de manière licite et pour un but précis et bien défini, sont nécessaires pour atteindre ce but et ne sont pas stockées pour une période dépassant le stricte nécessaire. Une intervention doit se limiter à l'envergure nécessaire et doit constituer le moyen le plus tempéré permettant d'atteindre le but.

Lorsque ces conditions préalables ont été remplies, c'est en principe l'article 8, paragraphe 1 de la loi DSG qui est applicable. À défaut d'autorisation ou d'obligation légale et si les intérêts vitaux de la personne concernée sont garantis, lorsque les données ne sont accessibles au public ou lorsqu'elles sont exploitées en majeure partie dans l'intérêt du donneur d'ordre, la personne concernée est obligée de donner son consentement. Quand il s'agit de données sensibles, l'article 9 de la loi DSG stipule des exigences encore nettement plus strictes.

Il convient de se conformer à ces obligations stipulées au droit de la protection des données dès le premier contact avec des données personnelles. Dans la pratique, il y a lieu d'obtenir un consentement à l'exploitation des données dans la plupart des cas, une information explicite sur la protection des données étant alors recommandée. Sur les sites web, en revanche, ceci peut se faire moyennant une case à cocher.

Fonction Tell-a-Friend

En Autriche, aussi, il faut se méfier de la publicité via des amis ; l'arrêt de la cour fédérale de justice BGH de 2013 peut servir de guide. En 2009 déjà, la cour suprême (Oberster Gerichtshof, OGH) [OGH 9/6/2009, 4 Ob 26/09s) s'est prononcée sur ce sujet et a qualifié de « système de boule de neige » un « programme de primes » proposé par un courtier d'assurance qui avait promis à ses clients le remboursement de leurs (propres) primes d'assurances s'ils lui rapportaient deux nouveaux clients pour la compagnie d'assurance. Les « systèmes de boule de neige » sont interdits en Autriche en vertu de l'article 27 de la loi sur la concurrence déloyale (UWG). De ce fait, le recours à ses propres clients risque d'être déloyal au moins dans des cas bien spécifiques.

Sanctions possibles

L'une des particularités autrichiennes, c'est l'article 109, paragraphe 3, point 20 de la loi TKG 2003 qui stipule une disposition de droit pénal administratif selon laquelle une violation de l'article 107, paragrphe 2 ou 5 de la loi TKG 2003 interdisant l'envoi de courriels ou de publicité directe est passible d'une peine pécuniaire pouvant atteindre 37 000,00 euros. En plus de préméditation, la simple négligence suffit pour entraîner des sanctions. La négligence est automatiquement présumée en cas de violation de la norme d'interdiction. Dans la pratique, cela signifie qu'un expéditeur doit lui-même apporter activement des preuves à sa décharge. À cet effet, il y a lieu d'invoquer des faits et d'apporter des preuves. Les affirmations d'ordre général ne suffisent pas pour contredire la négligence. La survenance d'un danger ou d'un dommage n'en est pas un prérequis. Une infraction récurrente est susceptible d'augmenter la peine pécuniaire stipulée à l'article 109, paragraphe 5 de la loi TKG 2003.

Comme en Allemagne, les sanctions peuvent englober également des droits à l'abstention ou aux dommages-intérêts. La réaction à des droits de ce type, notamment à des avertissements, est semblable à celle en Allemagne. Malgré cela, chaque cas requiert un examen et une appréciation de la part d'un expert compétent, étant donné qu'il existe malgré tout des divergences du droit allemand. Il y a notamment le risque que les frais à rembourser à la partie adverse soient plus élevés qu'en Allemagne.

Les personnes physiques tout comme les entreprises commerciales recevant les courriels peuvent invoquer un droit à la cessation résultant de l'article 354 de l'ABGB (Allgemeines Bürgerliches Gesetzbuch, code civil autrichien) qui repose sur l'atteinte générale à la personnalité perpétrée par une atteinte à la vie privée.

Ce sont notamment les entreprises concurrentes - des compétiteurs de l'expéditeur - qui sont susceptibles d'invoquer des droits contre l'expéditeur en vertu de l'article 14, paragraphe 1 en conjonction avec l'article 1 de la loi autrichienne fédérale sur la concurrence déloyale (Bundesgesetz gegen den unlauteren Wettbewerb, UWG) et demander une cessation et, en cas de culpabilité, des dommages-intérêts en vertu de l'article 16, paragraphe 1 de la loi UWG.

9. Notre recommandation : Certified Senders Alliance

La white list centrale « Certified Senders Alliance » (CSA) créée en 2003 par l'association eco - Verband der Internetwirtschaft e.V. et l'association allemande pour le marketing de dialogue, Deutscher Dialogmarketing Verband, propose une solution efficace pour les fournisseurs de services courriels (ESP) et les entreprises afin d'éviter les difficultés d'envois lors de leurs campagnes de courriel et d'améliorer la qualité du marketing par courriel. La white list garantit que les destinataires reçoivent effectivement les courriels qu'ils ont demandés ou dont ils ont besoin pour une transaction. Ce sont notamment les courriels de masse comme les newsletters, mais également les courriels de transaction (p. ex. les factures, les confirmations d'inscription, les confirmations de commande, etc.) qui atterrissent souvent dans le registre à pourriel (courriels appelés false positives) et restent ainsi en règle générale cachés à l'expéditeur, car les filtres à pourriels les font passer à la trappe, probablement par erreur. Ceci risque facilement de générer des pertes au niveau du chiffre d'affaire chez les entreprises concernées et une expérience fâcheuse chez l'utilisateur.

Grâce à la white list CSA, les ISP peuvent optimiser l'envoi de courriels reçus à leurs clients afin de continuer à protéger ces derniers de manière efficace contre les pourriels. Avec une certification CSA, les expéditeurs de courriels sont sûrs qu'ils se caractérisent comme sérieux et dignes de confiance vis-à-vis des ISP reliées à la CSA, évitant ainsi tout problème d'envoi en cas de réputation douteuse.

Les expéditeurs certifiés CSA se soumettent à des critères d'admission stricts. En plus, les prestataires de services certifiés transmettent, via leurs CGV, les critères CSA à leurs clients. Les critères d'admission requièrent la satisfaction de normes techniques et de contraintes juridiques exigeantes, élaborées par la CSA en coopération avec ses adhérents dans le cadre d'un processus permanent :

Les critères juridiques de la CSA sont conformes au droit en vigueur dans l'UE. Tout envoi de courriels commerciaux au sein des états membres de l'UE doit satisfaire à ces critères.

Les critères techniques ont été développés sur la base de retours d'expériences des ISP, des partenaires technologiques et des expéditeurs et sont ajustés en permanence afin de répondre aux exigences les plus récentes. La signature DKIM de tous les messages ainsi que l'utilisation de List Unsubscribe - Header, pour n'en citer que deux des critères techniques, sont exemplaires.

De plus, il y a un nombre de mécanismes sanctionnant les violations des règles en place commises par les expéditeurs. Le comité de réclamations et de certification (Beschwerde- und Zertifizierungsausschuss, BZA) surveille l'acceptation de nouveaux expéditeurs et le respect des règles. Les expériences faites à ce jour dans la pratique démontrent que les critères stricts paient. Chose réjouissante - le nombre des réclamations reçues - comparé au volume des envois des expéditeurs certifiés - est très faible. Dans des cas isolés, le BZA doit quand même infliger voire confirmer des sanctions

afin de maintenir la qualité de la white list. Ces sanctions aident à leur tour l'expéditeur concerné à identifier les points faibles dans ses propres processus ou de ceux de ses clients et à y remédier afin d'éviter tout problème majeur.

Afin de maintenir la grande qualité de la white list, la vérification juridique irréprochable et le contrôle de la gestion des réclamations ne suffisent pas, les critères techniques doivent également être vérifiés en permanence. Ainsi, les critères les plus importants exigés aux serveurs des courriels envoyés sont vérifiés chaque jour de manière automatisée et consignés dans un rapport. Ce rapport englobe également des tests complémentaires pour savoir si les serveurs des courriels ont été à l´origine de problèmes en raison de leur comportement d´envoi, ceci à la fois afin d'en informer les expéditeurs certifiés mais également pour obtenir des indices sur les problèmes lors des envois. Ici, il s'agit également d'une plus-value supplémentaire offerte par une affiliation à la CSA.

Depuis longtemps, la CSA s´est construite une solide réputation non seulement sur le marché national, mais également au niveau international et se réjouit, dès le début de son service opérationnel, d'une acceptation toujours croissante qui, elle, a un effet positif sur la croissance de la CSA. Exprimé en chiffres, la CSA englobe désormais plus de 100 ESP certifiés et d'autres entreprises établies dans 11 pays différents. D'autre part, les ISP reliés à la CSA couvrent plus de 500 millions de comptes courriels dans le monde entier. Par ailleurs, la CSA compte parmi ses adhérents des partenaires renommés de coopération et de la technologie qui continuent à élargir la portée de la CSA et mettent à sa disposition des instruments importants pour le monitorage des expéditeurs. Depuis des années, la CSA est la norme de qualité la plus connue et la plus répandue en Allemagne et désormais même au niveau mondial, représentant ainsi un grand succès pour l'économie internationale de l´internet.

La CSA propose également des prestations de services supplémentaires, comme des ateliers de travail où les experts donnent des stages aux responsables du marketing dans le domaine de la gestion du caractère délivrable et fournissent les conditions juridiques cadres pour les campagnes d´envois de courriels efficaces et conformes aux lois.

Vous trouverez une liste à jour des adhérents et des partenaires ainsi que toutes informations complémentaires sur la CSA sous **https://certified-senders.eu**.

10. Opt-In ou Opt-Out: les dispositions applicables dans les différents pays du monde

Au niveau de l'envoi international de courriels de publicité, l'expéditeur doit se poser la question fondamentale suivante : est-ce que le principe de l'opt-in (consentement préalable nécessaire) ou une règle opt-out (la possibilité de désabonnement suffit) est applicable dans le pays des destinataires (pays de destination) ? Car le point décisif pour l'appréciation de la licéité de l'action d'envoi, c'est la situation juridique dans le pays de destination concerné. L'opt-in est en vigueur dans tous les états membres de l'Union Européenne ainsi qu'en Norvège, au Liechtenstein, en Islande et en Suisse. Mais ceci n'est pas le cas partout dans le monde. La liste* ci-après répond à la question de l'applicabilité de l'opt-in ou de l'opt-out dans plus de 60 pays, classés par continents. Par ailleurs, la liste comporte pour la plupart des pays des informations importantes sur les bases juridiques y afférentes.

Europe

Pays	Opt-In	Opt-Out	Bases juridiques / commentaires
Allemagne	(+)		› German Civil Code (BGB) › Act Against Unfair Competition (UWG) › Telemedia Act (TMG) › Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG) › Consentement exprès nécessaire, exception pour les relations clients ; article 7, paragraphe 2, point 3, paragraphe 3 de la loi UWG › Aucune différence entre B2B ou B2C
Autriche	(+)		› opt-In pour le B2C et le B2B, exceptions pour les relations clients ; art. 107 paragraphe 2, paragraphe 3 de la TKR 2003, (modification 2006)
Belgique	(+)		› Law on Legal Aspects of the Services of the Information Society (loi du 11 mars 2003), › S´applique au B2C et B2B
Bulgarie	(+)		› Electronic Communications Act (Art. 261, paragraphe 1)
Chypre	(+)		› Section 06 of the Regulation of Electronic Communications and Postal Services Law of 2004
Croatie	(+)		› Zakon o elektroničkim komunikacijama, NN 73/08, 90/11, 133/12, 80/13, 71/14 "ZEK" › l'opt-out suffit pour le B2B (attention : sauf pour le contact non automatisé de personnes juridiques)
Danemark	(+)		

Pays	Opt-In	Opt-Out	Bases juridiques / commentaires
Espagne	(+)		› Information Society Services and › Electronic Commerce Act (34/2002 du 11 juillet) › Royal Decree 1720/2007 › La règle applicable aux consommateurs : l'opt-in est nécessaire, sauf si 1. l'adresse a été obtenue à l'occasion d'un achat au cours des 12 derniers mois 2. similitude des produits 3. possibilité opt-out gratuite et facilement compréhensible
Estonie	(+)		› Electronic Communications Act › pour le B2B, l'opt-out est suffisant
Finlande	(+)		› Finnish Information Society Code (Tietoyhteiskuntakaari 2014/917) (the "ISC") du 7 novembre 2014 › en vigueur depuis le 1er janvier 2015 › pour le B2B l'opt-out s´applique
France	(+)		› Law on Confidence in the Digital Economy (LECN) › La règle applicable aux consommateurs : l'opt-in est nécessaire, sauf si 1. l'adresse a été obtenue à l'occasion d'un achat au cours des 12 derniers mois 2. similitude des produits 3. possibilité opt-out gratuite et facilement compréhensible › pour le B2B, l'opt-out est suffisant
Grèce	(+)		› Law 3471/2006 (G.G. 133A'/28.06.06) "Protection of privacy and personal data in the telecommunications sector"
Hongrie	(+)		› Act No. XLVIII of 2008 on the Basic Conditions on and Restrictions of Commercial Advertising (the "Advertising Act")

Pays	Opt-In	Opt-Out	Bases juridiques / commentaires
Irlande	(+)		› Data Protection Act of 1998 › European Communities (Electronic Communications Networks and Services) (Data Protection and Privacy) Regulations 2003 (Statutory Instrument No. 535) de 2003) › Data Protection Act of 2003 (amending Data Protection Act of 1988) › La règle applicable aux consommateurs : l'opt-in est nécessaire, sauf si 1. l'adresse a été obtenue à l'occasion d'un achat au cours des 12 derniers mois 2. similitude des produits 3. possibilité opt-out gratuite et facilement compréhensible › pour le B2B, l'opt-out est suffisant (attention : uniquement pour les adresses courriels donnant l'impression d'être des adresses commerciales et uniquement pour la publicité dans ce domaine commercial)
Islande	(+)		
Italie	(+)		› Disposition anti-pourriel dans l'art. 130 de la loi italienne de la protection des données, Codice in materia di protezione dei dati personali › La règle applicable aux consommateurs : l'opt-in est nécessaire, sauf si 1. l'adresse a été obtenue à l'occasion d'un achat au cours des 12 derniers mois 2. similitude des produits 3. possibilité opt-out gratuite et facilement compréhensible
Lettonie	(+)		› pour le B2B, l'opt-out est suffisant
Liechtenstein	(+)		› Communication Act daté du 17 mars 2006, en vigueur depuis le 06 juin 2006
Luxembourg	(+)		
Lituanie	(+)		› Law on Electronic Communications (the "LOEC")

Pays	Opt-In	Opt-Out	Bases juridiques / commentaires
Malte	(+)		
Norvège	(+)		› Marketing Control Act, du 9 janvier 2009 › en vigueur depuis le 1er juin 2009
Pays Bas	(+)		› loi de télécommunication, loi fédérale de la protection des données ; en vigueur depuis le 1/10/2009 : The New Dutch Opt-In Law › pour le B2B et B2C : l'opt-in est nécessaire, sauf si 1. l'adresse a été obtenue à l'occasion d'un achat au cours des 12 derniers mois 2. similitude des produits 3. possibilité opt-out gratuite et facilement compréhensible
Pologne	(+)		
Portugal	(+)		› 2000/31/CE › Decree-Law 7/2004 (art. 22) › pour le B2B, l'opt-out est suffisant
Roumanie	(+)		
Royaume Uni	(+)		› Privacy and Electronic Communications (EC Directive) Regulations 2003 : › pour les consommateurs : l'opt-in est nécessaire, sauf si 1. l'adresse a été obtenue à l'occasion d'un achat au cours des 12 derniers mois 2. similitude des produits 3. possibilité opt-out gratuite et facilement compréhensible
Slovénie	(+)		› Slovenian Electronic Communications Act (Zakon o elektronskih komunikacijah, UL RS No. 109/2012, 110/2013) (the "ZEKom-1") › en vigueur depuis le 15 janvier 2013 › Electronic Commerce Market Act (Zakon o elektronskem poslovanju na trgu, UL RS No. 96/2009 and 19/2015) (the "ZEPT") › pour le B2B, l'opt-out est suffisant (depuis le 04 avril 2015)

Pays	Opt-In	Opt-Out	Bases juridiques / commentaires
Suède	(+)		› Swedish Marketing Act › pour le B2B, l'opt-out est suffisant
Suisse	(+)		› art. 3 de la loi fédérale sur la concurrence déloyale : › La publicité de masse par courriel n'est licite en Suisse qu'à condition qu'il est répondu aux prérequis suivants : 1. consentement préalable du client 2. divulgation de l'expéditeur effectif 3. information sur une possibilité de désabonnement gratuite et sans problème
Slovaquie	(+)		› Section 62 Act on Electronic Communications ("ECA") › en vigueur depuis le 1er novembre 2011
Tchéquie	(+)		› Act No. 480/2004
Ukraine	(+)		› pour le B2B, l'opt-out est suffisant

USA / Amérique du Sud / Canada

Pays	Opt-In	Opt-Out	Bases juridiques / commentaires
USA		(+)	› CAN-SPAM-ACT: Les points suivants constituent les contenus les plus importants de la loi (article 5) : l'expéditeur doit être identifiable 1. les objets induisant en erreur sont interdits, c'est-à-dire que l'objet ne doit informer le destinataire que du véritable contenu du courriel. 2. une option opt-out ou une possibilité unsubscribe doit être proposée 3. l'adresse postale de l'expéditeur doit être fournie
Argentine		(+)	› Personal-Data-Protection Act. › Il n'existe, certes, pas de loi exclusivement sur le marketing par courriel, mais l'article 27 de la Personal-Data-Protection comporte des dispositions relatives à la possibilité d'opt-out pour les courriels de publicité.

Pays	Opt-In	Opt-Out	Bases juridiques / commentaires
Brésil		(+)	› L'opt-in n'est, certes (pas encore) requise, mais utile, car il y a une tendance vers l'opt-in
Canada	(+)		› http://laws-lois.justice.gc.ca/eng/acts/E-1.6/index.html › depuis le 01/07/2014 : régime opt-in, rapprochement aux règles allemandes et loi anti-pourriel modifiée : Canada's Anti Spam Law (CASL); 1. consentement exprès donné par le destinataire à la réception du courriel de publicité avant l'envoi de celui-ci 2. aucun en-tête du message faux ou induisant en erreur (expéditeur ou objet) ; 3. aucune modification des données de l'envoi ; 4. un lien clairement visible voire repérable « lien de désabonnement » ; le courriel de publicité doit comporter l'adresse postale de l'expéditeur ; 5. aucune exploitation d'adresses courriel ayant été collectées de manière illicite.
Chili	(+)	(	
Colombie	(+)	(	
Costa Rica	(+)		
Mexique	(+)		
Pérou	(+)	(	
Vénézuela	(+)	(	› Consumer Protection Law

Afrique

Pays	Opt-In	Opt-Out	Bases juridiques / commentaires
Afrique du Sud	(+)		

Asie / Australie

Pays	Opt-In	Opt-Out	Bases juridiques / commentaires
Australie	(+)		› Spam Act 2003, un consentement exprès et préalable est toujours requis
Arabie Saoudite	(+)		
Bahreïn		(+)	
Chine	(+)		› China's Regulations on Internet Email Services 2006
Corée du Sud	(+)		› depuis novembre 2014
Dubai		(+)	
Émirats Arabes Unis	(+)		
Hong Kong	(+)		› Personal Data (Privacy) Ordinance (the "PDPO") qui comporte les Data Protection Principles (the "DPP") › pour le B2B, l'opt-out est suffisant
Inde			› aucun règlement du marketing par courriel
Indonésie	(+)		› Law No. 11 of 2008 on Electronic Information and Transaction («EIT Law»)
Israël	(+)		› Section 30A of the Telecommunications Act
Japon	(+)		› "New Anti-Spam Law" 2008, fort alignement aux principe européens
Malaisie	(+)		› pour le B2B, l'opt-out est suffisant
Nouvelle Zélande	(+)		› Unsolicited Electronic Messages Act 2007; › Privacy Act 1993
Philippines	(+)		
Russie	(+)		
Singapour		(+)	› Singapour a édicté la SPAM Control Act en 2007
Turquie		(+)	
Vietnam	(+)		

*en mai 2016 : les modifications des lois faites après cette date ainsi que la jurisprudence constante dans les différents pays n'ont pas été prises en compte. Dans certains pays, la désignation « B2B » peut se restreindre aux seules personnes morales. Information pour les expéditeurs CSA : un opt-in s'applique toujours, en conformité avec les règles CSA, afin de profiter des avantages d'un envoi optimisé et de répondre aux critères stricts des ISP.

Auteurs et relecture

Auteurs

Dr. Torsten Schwarz
Absolit Consulting und Email-Marketing Forum.de (propriétaire)
https://www.absolit.de

Christian Schmoll
Avocat, g3s Rechtsanwälte
www.g3s.legal,
Senior Counsel, Sprinklr, Inc.
www.sprinklr.com

Lukas Bühlmann
Avocat et partenaire,
Bühlmann Rechtsanwälte AG
http://www.br-legal.ch

Tamino Chochola
Stadler Völkel Rechtsanwälte GmbH
www.svlaw.at

Dr. Arthur Stadler
Avocat
Stadler Völkel Rechtsanwälte GmbH
www.svlaw.at

Martin Bucher
Directeur, Inxmail GmbH
www.inxmail.de

Dr. Jens Eckhardt
Avocat spécialisé dans le droit de la technologie d´information
Auditeur pour la protection des données (TÜV)
Derra, Meyer & Partner
www.derra.eu

Christan Solmecke
Avocat et partenaire
WILDE BEUGER SOLMECKE Rechstanwälte
www.wbs-law.de

Annika Dam
Avocate
WILDE BEUGER SOLMECKE Rechstanwälte
www.wbs-law.de

Ivo A. Ivanov
Avocat et conseiller judiciaire, eco e.V.

Rosa Hafezi
Avocate, département Professional Services, eco e.V.

Alexandra Koch-Skiba
Avocate, directrice du bureau des plaintes, eco e.V.

Qadir Rostamzada
Marketing & Business Development
eco e.V.

Relecture

Ivo A. Ivanov
Avocat, conseiller juridique, eco e.V

Rosa Hafezi
Avocate, département Professional Services, eco e.V.

Alexandra Koch-Skiba
Avocate, directrice du bureau des plaintes, eco e.V.

Dr. Katharina Küchler,
Avocate, département Professional Services, eco e.V.

Sebastian Fitting
Ass. jur., contact du bureau des plaints, eco e.V.

Peter Urlaub
Ass. jur., contact du bureau des plaints, eco e.V.

Traduction française assurée par
brigitte-cloot-translation.services

eco
Association de l'économie internet
Lichtstraße 43h
50825 Cologne
Télépone +49(0)221/700048-0
Télécopie +49(0)221/700048-111
info@eco.de
www.eco.de

www.certified-senders.eu

ASSOCIATION OF THE INTERNET INDUSTRY

WE ARE SHAPING THE INTERNET.

YESTERDAY. TODAY. BEYOND TOMORROW.

éditée par

CSA Certified Senders Alliance