
El marc legal de *l'email marketing*

PID_00272855

Xavier Folguera

Temps mínim de dedicació recomanat: 2 hores



Xavier Folguera

L'encàrrec i la creació d'aquest recurs d'aprenentatge UOC han estat coordinats per les professores: Cintia Pla Garcia, Iviane Ramos de Luna (2020)

Primera edició: març 2020
© Xavier Folguera
Tots els drets reservats
© d'aquesta edició, FUOC, 2020
Av. Tibidabo, 39-43, 08035 Barcelona
Realització editorial: FUOC

Cap part d'aquesta publicació, incloent-hi el disseny general i la coberta, no pot ser copiada, reproduïda, emmagatzemada o transmesa de cap manera ni per cap mitjà, tant si és elèctric com químic, mecànic, òptic, de gravació, de fotocòpia o per altres mètodes, sense l'autorització prèvia per escrit dels titulars dels drets.

Índex

| | |
|--|----|
| Introducció..... | 5 |
| 1. Lleis fonamentals: RGPD, LOPDGDD i LSSI..... | 7 |
| 1.1. Què és l'RGPD: definició | 7 |
| 1.2. Àmbit d'aplicació | 8 |
| 2. La captació de dades: principis i deures del nou reglament... | 9 |
| 2.1. El consentiment explícit | 9 |
| 2.2. El deure d'informar: informació per capes | 10 |
| 2.2.1. Primera capa: epígrafs bàsics | 10 |
| 2.2.2. Segona capa: document detallat | 12 |
| 2.3. El consentiment assegurat: el doble <i>opt-in</i> | 12 |
| 2.4. Els perfils segmentats | 12 |
| 2.4.1. La protecció de dades de menors de 14 anys | 13 |
| 2.4.2. La compra o cessió de bases de dades | 13 |
| 3. La gestió de dades en <i>email marketing</i>..... | 14 |
| 3.1. Els rols en la gestió | 14 |
| 4. Requeriments legals de l'<i>email</i>: revocació del consentiment. | 16 |
| 5. Els drets ARCO i la seva ampliació amb l'RGPD..... | 17 |
| 6. Transferència internacional de dades: eines d'enviaments.... | 19 |
| 7. Règim sancionador per incompliment de la llei..... | 20 |
| 7.1. Sancions | 20 |

Introducció

L'activitat de l'*email marketing* ha pres indiscutiblement el relleu del màrqueting directe per la seva economia i rapidesa, i també per la seva alta capacitat de segmentació, personalització i automatització. Aquesta disciplina publicitària que antany es canalitzava per mitjà del correu postal, avui es fa per mitjà del correu electrònic. El canvi en la comunicació directa entre l'empresa i el públic ha estat tan radical que el marc legal que empara els drets dels consumidors i les empreses s'ha hagut d'actualitzar aprofundint en aspectes dels drets a la privadesa de l'individu i les obligacions de les organitzacions en l'ús de les dades personals.

L'*email marketing* es basa fonamentalment en l'obtenció i la gestió de les dades, de la mateixa forma que antany, encara que d'una manera més profundament segmentada, gràcies al desenvolupament d'una societat cada vegada més digitalitzada. Per això, quan es planteja l'estudi o coneixement de la normativa que s'ha de complir, es pot comprendre millor si s'enfoca des de dues activitats diferents:

- 1) Des de la captació de les dades.
- 2) Des de la gestió de les dades i l'emissió de missatges, és a dir, en l'execució de campanyes massives publicitàries mitjançant el correu electrònic.

La norma actual ha posat molt èmfasi a dotar el ciutadà d'una eina que li atorgui la màxima seguretat en la protecció de la seva privadesa, ja que la circulació i l'accés a les dades personals és molt més intensa i assequible que en l'anterior, que era analògica.

Per això, com veurem, la normativa es basa especialment en els principis d'informar amb gran transparència per part de les empreses en el moment de la captació de les dades i del consentiment de l'usuari per a la recepció de missatges.

1. Lleis fonamentals: RGPD, LOPDGDD i LSSI

El marc legal que empara l'activitat de l'*email marketing* abasta diferents lleis i normes, entre les quals destaca el **Reglament general de protecció de dades (RGPD)**.

Aquesta norma constitueix un punt de referència clau per a l'activitat del màrqueting mitjançant el correu electrònic.

Amb aquesta norma, el ciutadà compta amb un marc legislatiu que pretén restringir l'ús de les seves dades personals, al mateix temps que es busca dotar les empreses de la suficient seguretat jurídica per a dur a terme activitats de màrqueting que defensin el dret a la informació de productes i serveis, tot això en un entorn de llibertat comercial i publicitària.

El 25 de maig de 2016 es va aprovar al Parlament Europeu el nou RGPD, el **Reglament (UE) 2016/679, general de protecció de dades**, una nova norma amb l'objectiu de protegir en el conjunt comunitari els drets dels ciutadans europeus pel que fa a les seves dades personals. Així doncs, tots els països de l'entorn comunitari es van veure obligats a adaptar les seves normes a l'aprovat al Parlament Europeu.

A Espanya també es va aprovar una llei complementària l'RGPD, després de la seva publicació en el *BOE* el 6 de desembre de 2018, amb el nom de **Llei orgànica de protecció de dades i garantia dels drets digitals (LOPDGDD)**. L'objectiu era adaptar la legislació espanyola a l'RGPD i regular el dret fonamental a la protecció de les dades.

Malgrat la preponderància d'aquestes lleis en l'*email marketing*, a Espanya també s'ha de tenir en compte el paper de la **Llei de la societat de la informació i del comerç electrònic (LSSI)**, llei que presenta articles vinculats a la protecció de les dades i a l'activitat de l'*emailing*, relacionats amb el dret a la revocació del consentiment per a les comunicacions comercials.

1.1. Què és l'RGPD: definició

El Reglament general de protecció de dades va ser aprovat al Parlament de la Unió Europea amb la finalitat d'harmonitzar les anteriors normatives de privadesa dels països de la UE i crear un marc de confiança per al desenvolupament

Vegeu també

La protecció de dades i l'activitat de l'*emailing* es tracta en l'apartat «Requeriments legals de l'*email*: revocació del consentiment» d'aquest mòdul.

del mercat únic digital. Aquesta confiança s'entenia des dels drets de protecció de les dades del ciutadà fins a la forma com les companyies havien d'afrontar la denominada *ciberseguretat*, tant en l'àmbit tècnic com organitzatiu.

L'RGPD és considerat com la norma més important de la Unió Europea quant a la protecció de les dades personals. Amb aquest s'ha dotat de major seguretat i control a les dades d'informació personal, i és d'obligat compliment des del 25 de maig de 2018 (dos anys després de la seva aprovació).

Com veurem, l'RGPD és una norma que es regeix per uns principis de transparència, de limitació d'ús, de minimització de les dades, de limitació en els terminis de conservació, d'integritat, seguretat i responsabilitat per part dels gestors de les dades.

1.2. Àmbit d'aplicació

L'RGPD s'aplica a qualsevol organització o empresa que processa dades de caràcter personal dels residents de la Unió Europea o que té el seu establiment permanent a la UE, o a empreses els serveis o productes de les quals són comercialitzats als ciutadans que resideixen allí. Quan parlem de dades personals ens referim a les de qualsevol persona física, tant en el rol de client o consumidor, com en el de treballador d'una empresa.

2. La captació de dades: principis i deures del nou reglament

En la captació de dades hi ha dos grans principis en el compliment de la llei: el **consentiment explícit de l'usuari** i el **deure d'informar**.

Tots dos constitueixen els factors diferencials sobre les anteriors normatives i, per això, les empreses han hagut d'actualitzar els seus procediments per continuar realitzant l'*email marketing*. Les dades aconseguides amb els anteriors procediments, mitjançant permís tàcit i sense informar, no es poden utilitzar.

2.1. El consentiment explícit

El primer concepte fonamental que distingeix aquesta norma pel que fa a les anteriors lleis és l'obligació de poder demostrar de manera fefaent i demostrable la captació de dades sol·licitant el consentiment de l'usuari, és a dir, obtenint el seu beneplàcit explícit.

Les empreses han de disposar de la tecnologia necessària per poder demostrar a l'Administració i als titulars de les dades, en qualsevol moment, que han rebut aquestes dades de forma lícita (per la qual cosa han de disposar d'un arxiu o document acreditatiu) i, al mateix temps, que ofereixen a l'usuari la revocació d'aquest consentiment de manera fàcil i gratuïta.

Per tant, qualsevol recopilació de dades s'ha d'obtenir amb la voluntat de l'usuari de forma expressa i lliure, és a dir, s'exclou el consentiment tàcit, com succeïa anteriorment. Aquesta recopilació ha d'estar enfocada a una finalitat concreta i declarada prèviament, i s'impedeix el seu ús a qüestions alienes. L'usuari podrà saber quin ús s'està fent de les seves dades, o sigui, serà verificable.

Cal matisar que, en el cas de les comunicacions als clients actuals, no cal el consentiment explícit del destinatari per a l'enviament d'informacions de productes o serveis que van originar la relació comercial existent. Això és així atès que l'enviament pot entrar dins de les expectatives raonables del client, per la qual cosa té la base legítima en l'interès legítim del responsable.

2.2. El deure d'informar: informació per capes

La llei obliga les empreses a informar els ciutadans sobre l'ús que es farà de les seves dades personals prèviament a la seva cessió. En l'*email marketing*, una dada personal fonamental és l'adreça de correu electrònic, i es considera com a tal tant en l'àmbit particular com professional.

Aquesta obligació de transparència en la captació de dades s'ha d'aplicar a qualsevol tipus de suport, sigui físic, digital o oral, o sigui, en versió paper, versió en línia, versió telefònica, fins i tot, als nous suports tecnològics (IoT) i aplicacions mòbils.

En l'antiga norma, ja s'exigia que s'informés sobre l'existència d'un fitxer, una finalitat, els destinataris i la possibilitat d'exercir els drets d'accés, rectificació, cancel·lació i oposició, però el nou RGPD afegeix requisits addicionals quant a informar les persones interessades. Els nous requisits principals són l'obligació d'informar sobre la base jurídica o legitimació per al tractament, les dades del delegat de protecció de les dades, els terminis i criteris de conservació de les dades i altres més detallats, que s'han de transmetre en les denominades *capes d'informació*.

L'RGPD preveu l'existència del redactat d'un document, freqüentment denominat *Política de privadesa*, que qualsevol organització ha de posseir per informar sobre els punts abans esmentats, i que s'ha de presentar a l'usuari que cedeix les dades, mitjançant dos tipus de capes d'informació: una primera capa d'epígrafs resumits i una segona capa amb el document complet.

Epígrafs

Els **epígrafs** són els conceptes fonamentals presentats de forma resumida que són desenvolupats en un document més extens situat al lloc web on es capten les dades.

2.2.1. Primera capa: epígrafs bàsics

L'objectiu de la norma és que l'usuari pugui llegir fàcilment una informació bàsica sobre l'ús que es farà de les seves dades en el moment de cedir-les, i obliga les empreses que desitgen obtenir-les al fet que informin en una primera «capa d'informació» –per mitjà d'una taula amb un resum en forma d'epígrafs bàsics– del conjunt de les informacions requerides per la llei.

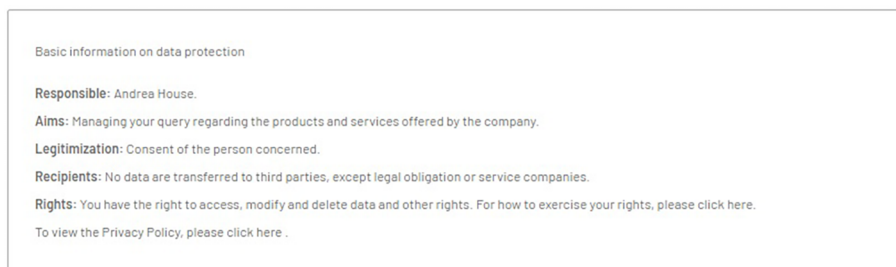
Aquests epígrafs es refereixen al responsable, la finalitat, la legitimació, el destinatari i els drets.

Aquest petit resum informatiu s'ha d'acompanyar d'una casella d'acceptació (*check box*), que l'usuari ha de marcar abans de cedir les dades, la qual cosa confirma l'acceptació de la cessió de les dades i l'empresa que les capta acon-

segueix la seguretat jurídica per l'acceptació explícita de l'usuari. D'aquesta manera, es resol el primer principi exposat sobre el consentiment explícit del cedent de les dades.

Al mateix temps, a més del *check box* abans esmentat, hi ha d'haver un enllaç (hipervincle) dirigit al gruix de la informació, la denominada «segona capa» d'informació, més detallada i completa. L'usuari ha de declarar que ha llegit aquest document i que ha estat informat prèviament a la seva cessió. Tot això dota el concepte **tractament de dades** d'un sentit molt major al que se li atorgava anteriorment.

Imatge 1. Exemple d'epígrafs bàsics



Responsable. Es denomina responsable del tractament de dades a l'entitat o empresa propietària de la base de dades. S'haurà d'exposar el nom de l'empresa que és responsable de la base de dades. Aquesta empresa pot cedir-les a un «encarregat» i pot tenir un delegat, com veurem més endavant.

Finalitat. S'han d'exposar amb transparència les finalitats del tractament, és a dir, per a què s'utilitzarà la base de dades. També s'explicitaran els terminis i els criteris de conservació, a més de l'existència de missatges automatitzats i de perfils segmentats d'usuaris.

Legitimació. S'ha de detallar la base jurídica del tractament, això és, si hi ha obligació o voluntarietat en la cessió de dades. Habitualment, es manifesta el simple consentiment voluntari de l'usuari.

Destinatari. Aquest punt es refereix a la intenció de possibles cessions o transferències de dades a tercers. Per exemple, si l'empresa forma part d'un grup d'empreses amb activitats diferents, ha de quedar explicitat si cedirà les dades o no.

Drets. S'exposa l'exercici dels drets d'accés, supressió, portabilitat i oposició. També s'ha de concretar la forma de poder exercir aquests drets.

2.2.2. Segona capa: document detallat

El document que desenvolupa els epígrafs habitualment es denomina *Política de privadesa* i expressa la forma com cada empresa o organització cuida i processa les dades de l'usuari, mantenint la informació obtinguda amb garanties.

Cada organització té el seu propi document, ja que no hi ha un model prefixat amb exactitud. És responsabilitat de l'usuari llegir-lo abans d'acceptar-lo per assegurar-se que no hi hagi condicions que incloguin el risc d'intercanvi d'informació o qualsevol altra clàusula que es pugui interpretar com una violació de la seva privadesa.

2.3. El consentiment assegurat: el doble *opt-in*

Una de les eines recomanades en la captació segura de dades és l'ús del **doble *opt-in***. Aquest mecanisme consisteix en l'enviament d'un missatge a la safata d'entrada del titular de les dades després d'haver donat la seva adreça de correu i acceptat el seu registre a la base de dades. Aquest missatge inclou un enllaç que ha de ser confirmat per l'usuari per donar validesa al seu registre en la base de dades.

Si bé és cert que quan un usuari introdueix la seva adreça de correu en un formulari, amb un *opt-in* simple pot quedar constància que s'ha registrat, pot donar-se la circumstància que l'adreça sigui errònia o d'un altre usuari, la qual cosa impossibilita que l'usuari confirmi la seva adreça i, per tant, no queda realment registrat a la base de dades. Per això, la via més segura és el doble *opt-in*.

Així doncs, l'empresa podria disposar d'un arxiu informàtic de doble *opt-in* amb les dades del registre, i també del correu comunicat per l'usuari, la qual cosa la dotaria d'una completa documentació que, en cas de litigi, avalaria l'empresa davant un organisme competent, que sempre es regirà pel principi de la demostració.

2.4. Els perfils segmentats

L'èxit de l'*email marketing* es basa en la segmentació dels perfils personals amb les dades obtingudes. Aquesta segmentació es pot realitzar o processant les dades i agrupant-les segons els interessos de l'usuari, o des dels interessos de l'empresa. Amb això, les empreses poden crear perfils de persones i usar-los per avaluar determinats aspectes vinculats amb aquestes.

L'objectiu final de la segmentació és intentar predir el comportament humà i prendre decisions estratègiques i tàctiques, la qual cosa implica freqüentment el tractament automatitzat de les dades. Amb els perfils segmentats, qualsevol empresa pot decidir a quins grups pot o ha de fer enviaments amb missatges específics per augmentar l'eficàcia de cada campanya.

La normativa actual permet tot tipus de creació de perfils, però les empreses han d'assegurar drets importants a les persones que formen part d'aquestes bases.

- Sol·licitar el consentiment previ i explícit per a dur a terme les operacions d'anàlisi del comportament dels usuaris.
- El dret a l'oblit. Si l'usuari desitja que s'esborrin dades concretes, l'empresa ha de dur a terme aquesta supressió.
- El dret a ser informat i a posseir una còpia de les seves dades personals.
- El dret d'oposició i d'interrupció del tractament.

2.4.1. La protecció de dades de menors de 14 anys

Els perfils humans segmentats que inclouen menors requereixen una especial atenció. Les empreses que venen productes enfocats a menors, com ara joguines, aplicacions o videojocs, hauran d'obtenir el consentiment d'alguns dels progenitors si desitgen recaptar dades sobre les seves preferències, interessos o gustos. Per això, hauran d'oferir una informació més clara, senzilla i transparent.

Igual que amb la resta de segments de la població, les empreses estan obligades a emmagatzemar proves que comptin amb el consentiment dels pares i, en definitiva, de tots els contactes inclosos en la base de dades.

2.4.2. La compra o cessió de bases de dades

L'RGPD permet teòricament l'adquisició de llistes de contactes, sempre que el consentiment s'hagi donat de manera clara i sigui demostrable, però a Espanya, l'actual Llei orgànica de protecció de dades impedeix la transferència del consentiment i, en conseqüència, no és legal adquirir o usar llistes d'altres.

Dit en altres paraules, encara que puguem obtenir de tercers correus electrònics d'usuaris, no per això hem adquirit el consentiment de l'usuari per enviar-li un correu que no ha autoritzat explícitament.

3. La gestió de dades en *email marketing*

L'*email marketing* és l'eina de màrqueting digital més antiga de les existents i ha estat utilitzada per les empreses des de l'inici d'internet. Durant molt temps i en general, les organitzacions han recaptat dades de forma tàcita, o sigui, sense obtenir un consentiment exprés de l'usuari, però el nou marc normatiu ha obligat a la revisió dels processos, processos en què intervenen no solament empreses i usuaris, sinó també agències de màrqueting digital o empreses externes.

Per això, la nova llei ha descrit nous actors en la pràctica professional de l'*email marketing*, que serveixen per elevar el nivell de control en la protecció de dades del ciutadà i per repartir-se les responsabilitats en el compliment de la llei.

3.1. Els rols en la gestió

La nova llei descriu amb claredat els tres rols que intervenen en aquesta pràctica professional i exigeix a cadascun d'aquests unes responsabilitats específiques que no es poden passar per alt.

1) Responsable

El **responsable del tractament** descrit en l'RGPD és la persona física o jurídica que determina les finalitats i mitjans del tractament de les dades.

Podem parlar de l'empresa, l'autònom o la persona física que duu a terme activitats comercials i que retrà compte d'aquestes a les autoritats i a l'usuari en cas de conflictes.

El responsable decideix l'ús que es farà de les dades, la seva conservació, la seva cessió o si s'eliminaran. En resum, estarà obligat al deure d'informar, guardar secret, comprovar que les dades siguin correctes i autèntiques, que s'han obtingut de forma lícita i comprovable, atenent els ciutadans en el seu dret d'accés, rectificació i cancel·lació, adoptant totes les mesures possibles de seguretat organitzativa.

2) Encarregat

Les empreses confien en tercers per gestionar moltes activitats que impliquen la transmissió de dades personals, com poden ser assessories laborals o mútues mèdiques, en què pel que fa a l'*email marketing*, hi poden intervenir agències digitals que realitzin campanyes d'*email marketing*. Aquest rol es denomina *encarregat*.

Quan una companyia encarrega a tercers la realització de tractaments, aquesta relació ha de quedar regulada en un contracte escrit en què consti que l'encarregat complirà un conjunt de requisits:

- Es limitarà a utilitzar les dades exclusivament per a la finalitat descrita i no per a altres finalitats.
- Mantindrà absolut secret sobre el contingut de la base de dades.
- Tractarà les dades d'acord amb les instruccions del responsable del tractament.
- Exposarà les mesures de seguretat que l'encarregat estarà obligat a complir.

L'existència d'aquest contracte permet a l'encarregat l'accés a les dades dels usuaris sense el permís d'aquests, ja que se suposa que el responsable ha cedit aquest dret. Finalment, l'encarregat del tractament ha de retornar les dades o eliminar-les quan ha finalitzat el servei contractat.

3) Delegat

La nova llei incorpora una nova figura en el tractament de dades, denominada *delegat de protecció de dades*. L'existència d'aquesta figura solament és obligada o a empreses les activitats principals de les quals requereixin un control o una observació freqüent i sistemàtica de les dades de persones a gran escala, o que s'incloguin en el tractament dades de categories especials.

Alguns dels tipus d'empreses obligades a nomenar un delegat són les empreses prestadores de serveis de la societat de la informació que elaborin perfils, les que desenvolupin publicitat i prospecció comercial, o sigui, agències digitals que gestionen dades de consumidors en nom d'un anunciant. Hi ha moltes més empreses obligades, com ara les vinculades a la docència, inversió, sanitat i joc en línia, entre d'altres.

Entre les funcions del **delegat**, destaquen la supervisió del previst en l'RGPD, l'assessorament al responsable o encarregat i la seva cooperació amb l'autoritat de control (Agència Espanyola de Protecció de Dades), en cas necessari.

4. Requeriments legals de l'*email*: revocació del consentiment

En qualsevol campanya d'*email marketing*, és imperatiu legal que tots els missatges incloguin enllaços per a la fàcil revocació del consentiment de l'usuari per a la recepció de comunicacions comercials.

L'article 22.1 de la Llei de serveis de la societat de la informació regula aquesta obligació.

«[...] els prestadors de serveis hauran d'habilitar procediments senzills i gratuïts perquè els destinataris dels serveis puguin revocar el **consentiment** que hagin prestat. Quan les comunicacions hagin estat enviades per **correu electrònic** aquest mitjà haurà de consistir necessàriament en la inclusió d'una adreça de correu electrònic o una altra adreça electrònica vàlida on es pugui exercitar aquest dret, quedant prohibit l'enviament de comunicacions que no incloguin aquesta adreça.»

Article 22.1 de la Llei de serveis de la societat de la informació.

Dit d'una altra manera, l'usuari ha de poder **revocar el seu consentiment** per rebre **comunicacions comercials** utilitzant la mateixa comunicació, per exemple, mitjançant un enllaç al peu del missatge, esmentant «donar-se de baixa» o «dessubscripció».

5. Els drets ARCO i la seva ampliació amb l'RGPD

Hi ha quatre drets en la LOPDGDD que qualsevol usuari pot exercir per protegir les seves dades de caràcter personal: el dret d'accés, el dret de rectificació, el dret de cancel·lació i el dret d'oposició (ARCO). Cada dret resol una necessitat diferent:

- **Dret d'accés.** Permet a l'interessat conèixer les dades que s'estan processant i la finalitat, l'origen i les comunicacions en les quals està present.
- **Dret de rectificació.** L'usuari pot exigir canvis per errors.
- **Dret de cancel·lació.** Permet l'exigència de retirada i arxiu de dades, si l'interessat ho considera inadequat.
- **Dret d'oposició.** Sempre que alguna norma legal no digui el contrari, l'usuari té el dret a oposar-se al tractament de les seves dades quan no sigui necessari el seu consentiment.

Amb l'entrada en vigor de l'RGPD, a aquests quatre drets se li han sumat altres tres, que certament poden ser més circumstancials que els anteriors des del punt de vista de l'*email marketing*:

- **Dret d'oblit.** Permet a l'interessat exigir no solament la retirada del permís i arxiu de dades, sinó directament la supressió de les dades. Aquest dret es pot exercir en múltiples casos, com, per exemple, la retirada del seu consentiment o el compliment d'una obligació legal.
Es dona la circumstància que les empreses també es podrien negar a eliminar aquestes dades en certs casos, com per exemple quan està protegit pel dret a la llibertat d'expressió o quan aquestes dades són usades per a finalitats d'arxiu d'interès públic o estadístiques.
- **Dret de portabilitat.** D'acord amb el que disposa el citat article 20 de l'RGPD, l'interessat té dret a «rebre les dades personals que li incumbeixin, que hagi facilitat a un responsable del tractament, en un format estructurat, d'ús comú i lectura mecànica, i a transmetre-les a un altre responsable del tractament sense que ho impedeixi el responsable al qual les hi hagués facilitat».
Es pot dir que s'aplica el dret de la portabilitat en telefonia en el terreny de les dades personals. En definitiva, el dret a la portabilitat té per objecte atribuir a l'interessat un major control sobre les seves dades personals i afavorir el lliure flux de dades personals a la UE amb la finalitat de fomentar la competència.

- **Dret de limitació del tractament** (article 18 RGPD). L'RGPD augmenta la capacitat de decisió i control dels ciutadans sobre les seves dades personals. Limitar el tractament significa que, si l'interessat vol esborrar les seves dades personals però algun motiu legal ho impedeix, aquest pot sol·licitar la limitació de les seves dades al responsable del tractament. D'aquesta manera, les dades poden ser conservades, però no utilitzades per a altres finalitats.

6. Transferència internacional de dades: eines d'enviaments

Amb l'entrada en vigor de l'RGPD, el legislador europeu també ha volgut protegir el dret a la protecció de les dades personals més enllà de la Unió Europea. En aquest sentit, moltes de les eines *cloud* (al núvol) que utilitza l'*email marketing* estan allotjades en servidors de fora de l'entorn europeu, per la qual cosa podria estar incomplint la llei.

Els països que estan fora de les fronteres europees han de garantir nivells de garantia o adequació en matèria de protecció de dades equivalents als establerts a la Unió Europea. En el cas de les companyies americanes, si estan adherides a l'acord EU-US Privacy Shield, és suficient, i aquest és el cas de Mailchimp.

Amb l'RGPD, les transferències internacionals de dades han d'estar controlades.

Es defineix com a **transferència internacional** qualsevol comunicació de dades personals que es produeix entre un responsable o encarregat situat en un país membre de la UE, i un encarregat o responsable situat fora d'aquest.

Amb l'entrada en vigor de l'RGPD, qui exporti dades, sigui l'encarregat o el responsable del tractament (per exemple, una agència digital o el mateix anunciant), assumeix responsabilitats en cas de conflicte. Per tant, la nova llei atribueix responsabilitat als proveïdors de les empreses com ara els encarregats i les mateixes companyies propietàries de les bases de dades com a responsables d'aquestes.

En general, l'RGPD no exigeix aprovació de l'autoritat de control (Administració) per realitzar legítimament una transferència internacional de dades, excepte en alguns casos especials inclosos en l'article 43 LOPDGDD. En altres paraules, es pot utilitzar qualsevol eina d'*email marketing*, sempre que al país de recepció s'ofereixin garanties adequades, mitjançant l'aprovació de les denominades *normes corporatives vinculants*. Aquestes normes són el model de referència de la UE sobre la privadesa de les dades.

7. Règim sancionador per incompliment de la llei

Les infraccions de protecció de les dades es divideixen en lleus, greus i molt greus.

Taula 1. Exemples d'infraccions

| Lleus | Greus | Molt greus |
|--|---|---|
| <ul style="list-style-type: none"> La falta de transparència de la informació. L'incompliment d'informar l'afectat quan ho hagi sol·licitat. L'incompliment de les obligacions de l'encarregat. | <p>Les infraccions greus són la que vulnereu substancialment el tractament i estan relacionades amb:</p> <ul style="list-style-type: none"> L'obtenció o l'ús de dades d'un menor d'edat recaptades sense consentiment. La falta d'adopció de mesures tècniques i organitzatives necessàries per a l'efectiva protecció de les dades. L'incompliment de nomenar un responsable o encarregat del tractament de les dades. | <p>Les infraccions molt greus impliquen un incompliment substancial del tractament:</p> <ul style="list-style-type: none"> L'ús de les dades per a una finalitat diferent a la pactada. L'omissió del deure de la correcta informació a l'afectat. L'exigència d'un pagament per poder accedir a les dades pròpies emmagatzemades. La transferència internacional d'informació sense garanties. |

Els **infractors** poden ser:

- 1) Els responsables dels tractaments.
- 2) Els encarregats dels tractaments.
- 3) Els representants dels responsables o encarregats dels tractaments no establerts al territori de la Unió Europea.
- 4) Les entitats de certificació.
- 5) Les entitats acreditades de supervisió dels codis de conducta.

7.1. Sancions

L'import marcat en l'RGPD per l'incompliment de la norma abasta les infraccions greus i molt greus:

- Les **infraccions greus** se sancionaran amb multes administratives que poden ascendir fins als deu milions d'euros o, si es tracta d'una empresa, una quantia màxima del 2% de la facturació.
- Les **infraccions molt greus** se sancionaran amb multes administratives que poden ascendir als vint milions d'euros o, tractant-se d'una empresa, d'una quantia equivalent al 4% de la facturació.