TÉCNICO LISBOA

# O novo paradigma do Regulamento Geral de Protecção de Dados e o Impacto na *Cloud*

**Cátia S. Guerreiro Dionísio**

Dissertação para obtenção do grau de Mestre em:

## Segurança da Informação e Direito do Ciberespaço

Orientadores:

Prof. Doutor Carlos Caleiro
Prof. Doutor Alexandre Sousa Pinheiro

### Júri

Presidente: Professor Paulo Mateus
Orientador: Professor Jose Alexandre Sousa Pinheiro
Vogal: Professora Ana Fouto

**Outubro 2018**

# Agradecimentos

A presente dissertação de mestrado não poderia chegar a bom porto sem o precioso apoio de várias pessoas.

Em primeiro lugar, não posso deixar de agradecer ao meu orientador e co-orientador, Professor Doutor Carlos Caleiro e Professor Doutor Alexandre Sousa Pinheiro. Expresso o meu profundo agradecimento pela orientação e apoio incondicionais que muito elevaram os meus conhecimentos científicos, e sem dúvida, muito estimularam o meu desejo de querer, sempre, saber mais e a vontade constante de querer fazer melhor.

Desejo igualmente agradecer a todos os meus colegas do Mestrado em Segurança da Informação e Direito do Ciberespaço pelo apoio e amizade que estiveram presentes em todos os momentos.

À minha família e amigos, em especial aos meus país, um enorme obrigada por acreditarem sempre em mim e naquilo que faço e por todos os ensinamentos de vida. Espero que esta etapa, que agora termino, possa, de alguma forma, retribuir e compensar todo o carinho, apoio e dedicação que, constantemente, me oferecem. Também aos meus amigos, pelas revisões incansáveis ao longo da elaboração desta dissertação.

O meu profundo e sentido agradecimento a todas as pessoas que contribuíram para a concretização desta dissertação, estimulando-me intelectual e emocionalmente.

“When it comes to privacy and accountability, people always demand the former for themselves and the latter for everyone else.”
— **David Brin**

A presente tese foi escrita
segundo o antigo acordo ortográfico.

# Abstract

The recent digital era has given rise to an exceptionally high degree of personal data and information sharing. This has led to many countries being faced with the debate, and concern, of going about protecting rights, especially those concerning personal individual rights. Recently, the European Union has also dedicated itself to enhance the Data Protection right, having its state of art with the implementation of the General Data Protection Regulation (GDPR).

With the rise of cloud computing, the problem concerning geographical location of the several infrastructures which house data has emerged, especially in regards to the fact that data is stored across countries within the E.U and 3rd part countries. The European Commission now has to deal with how to analyze and protect personal information within the realm of the GDPR.

While the transmission of data across frontiers is one of the main preoccupations relating to cloud computing, it is important to highlight the role that Cloud Service Providers play, these entities assumed less responsibilities due to Directive 95/46/CE, however, with the GDPR, they are now seeing their respective responsibilities shifting.

This thesis aims to summarize the thesis and to showcase several problems that have arisen in regards to the protection of data when it crosses frontiers to 3rd party countries as well as to analyze the responsibility which Cloud Service Providers have in protecting these personal rights be it or as a processor.

# Resumo

A nova era digital levou a uma exponencial troca de dados e informação pessoal. Desde há muito que os Estados demonstraram uma preocupação em proteger a informação com um especial enfase na informação pessoal. Sendo que a União Europeia tem também ela se dedicado à protecção de dados, tendo como estado de arte o Regulamento Geral de Protecção de dados.

Desde o aparecimento da computação em cloud que se levantou o problema da localização geográfica das infra-estruturas estar dispersa em vários pontos geográficos trouxe assim problemas no que toca fluxos transfronteiriços, mais ainda no que toca a fluxos para países terceiros à União Europeia. Jaz na Comissão Europeia a competência para analisar a transmissão de dados pessoais para outros países terceiros, de forma a avaliar o nível de adequação desses Estados com o regulamento.

Ao mesmo tempo que os fluxos transfronteiriços são uma das preocupações principais quando pensamos em cloud também é de relevar o papel dos Could Service Providers, que assumiam anteriormente responsabilidades mínimas com a Directiva 95/46/CE mas que com o Regulamento Geral de Protecção de dados ve as suas responsabilidades alteradas.

Desta forma a presente tese foca-se na problemática da protecção de dados aquando da transferência para países terceiros bem como na responsabilidade que têm os *Cloud* Service *Providers* na protecção dos dados pessoais dos titulares, seja como Responsáveis pelo Tratamento dos Dados seja como Subcontratantes.

# Palavras-Chave
# Keywords

## Palavras-Chave

Computação em *Cloud*

Dados Pessoais

Provedores de Serviços de *Cloud*

Protecção de dados

Regulamento geral de protecção de Dados

Transferência de dados

## Key-Words

*Cloud Computing*

Data Protection

Data Transference

General Data Protection Regulation

Personal Data

*Cloud Service Provider*s

**INDICE**

# List of Figures

## Lista de Abreviaturas

**ARPA** - Advanced Research Projects Agency

**Art.** -(arts.) Artigo(s)

**CERN** - Conseil Européen pour la Recherche Nucléaire

**CEDH** - Convenção Europeia dos Direitos do Homem

**Convenção 108-** Convenção para a Protecção das Pessoa relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal do Conselho da Europa.

**Directiva** – Directiva 95/46/CE, de 24 de Outubro de 1995

**HTTP** - Hypertext Transfer Protocol

**IBM –** Intelligence Business Machine Corporation

**IaaS –** Infrastruture as a *Service*

**IP** – Internet Protocol

**IRC** - Internet Relay Chat

**MIT**- Massachusetts Institute of Technology

**OCDE** - Organização para Cooperação e Desenvolvimento Económico

**NIST -** National Institute of Standards, Information Technology Library

**ONG** – Organização Não Governamental

**P.** – Pagina

**PP.-**Paginas

**RGPD** – Regulamento Geral de Protecção de Dados

**SaaS –** Sofware as a *Service*

**TI** – Tecnologias da informação

**UE** – União Europeia

**EUA** – Estados Unidos da América

**WWW** – World Wide Web

**PaaS –** *Platform* as a *Service*

# 1 Introdução

A informatização de todos os serviços, uma inevitável realidade depois da evolução tecnológica a que se tem vindo a assistir nas últimas décadas, trouxe grandes benesses, desde a cada vez menos utilização do papel à rapidez de acesso de informação a partir de qualquer ponto do globo. Uma aldeia global na qual se pode exercer livremente o direito de informar e ser informado. Esta evolução das novas tecnologias que promove uma cada vez maior e mais rápida recolha de dados, acarreta em si uma necessidade da criação de legislação.

## 1.1 Motivação

O Direito à privacidade merece protecção especial no que diz respeito ao meio virtual, devido à maior amplitude de propagação. A Carta Universal dos Direitos do Homem no seu artigo 12º diz-nos que "*Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a protecção da lei.*"[1]. Assim, e tendo em conta a especial velocidade de propagação de informação no ciberespaço, há aqui uma necessidade de promover a protecção de dados.

O problema surge quando nos confrontamos com uma movimentação dos dados. Este paradigma torna-se ainda mais relevante quando entramos na esfera da computação em nuvem, ou seja, a *cloud computing*. Segundo o *National Institute of Standards and Technology* (NIST), a computação em nuvem é um modo que permite o acesso ubíquo, conveniente, a pedido e através de uma rede, a um conjunto de recursos computacionais configuráveis (por exemplo, redes, servidores, armazenamento, aplicações e serviços), que podem ser rapidamente disponibilizados e fornecidos com um esforço mínimo de gestão ou interacção mínima com o prestador de serviços.[2]

[1] Carta Universal dos direitos do homem, art 12º.

[2] "The NIST Definition of Cloud Computing", National Institude of Standards and Tecnlogoly p.5 disponível em https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpúblication800-145.pdf, acedido pela ultima vez a 4 de Maio de 2018.

Em suma a computação em *cloud* é um serviço de armazenamento de dados, sendo que, a diferença deste sistema para as anteriores formas de armazenamento de dados, é que diferentemente do *compact disc* ou de discos rígidos, a *cloud* tem a sua base na internet, ou seja, se anteriormente as pessoas utilizavam programas ou *softwares* que tinham de estar instalados num computador físico ou num servidor, hodiernamente a computação em *cloud* permite que as pessoas acedam às suas informações a partir de qualquer ponto desde que exista uma conexão à internet.

Desta forma, foi havendo uma crescente preocupação em proteger os dados pessoais nomeadamente também no que concerne à sua transferência. A UE assumiu esta preocupação desde há alguns anos, a Directiva 95/46/CE[3] e o novo Regulamento Geral de Protecção de Dados[4] fazem transparecer essa preocupação.

## 1.2 Contribuições

A presente tese foca-se na problemática da protecção de dados aquando da transferência para países terceiros bem como na responsabilidade que têm os *Cloud Service Providers* na protecção dos dados pessoais dos titulares, seja como Responsáveis pelo Tratamento dos Dados seja como Subcontratantes.

Como principais contribuições, estas serão fornecer um documento para futuro enquadramento do Regulamento Geral de Protecção de Dados com o papel e responsabilidades dos *Cloud Service Providers*, fazer uma análise compreensiva da literatura existente sobre o impacto do novo regulamento nos CSP e finalmente a presente dissertação tem ainda como objectivo contribuir, com base em toda a análise feita, com uma opinião sobre o papel desempenhado pelo CSP enquanto subcontratante ou responsável pelo tratamento de dados.

[3] Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

[4] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados

## 1.2 Organização

A presente dissertação está organizada em oito capítulos. O primeiro capitulo é constituído pela presente introdução, na qual são traçados o âmbito do estudo e objectivos.

No capítulo segundo será descrita a evolução histórica, tanto a nível de formação do regime jurídico europeu de protecção de dados pessoais, como também do desenvolvimento tecnológico da internet e da computação em *cloud*.

No terceiro capítulo será feito um enquadramento tecnológico, explicando os vários modelos de computação em *cloud*. Primeiramente os modelos de serviço de *Cloud Computing*, ou seja, *Cloud* como *Infrastructure as a service*, *Platform as a service e sofware as a service*. No que concerne aos modelos de desenvolvimento, foram abordados os conceitos de *cloud* privada, *cloud* pública, *cloud* comunitária e *cloud* híbrida.

No capítulo quarto realizar-se-á um estudo da legislação em vigor na União Europeia no que diz respeito à protecção de dados, ou seja, o Regulamento Geral do Protecção de dados, dando ênfase às definições de dado pessoal e categorias especiais de dados bem como ao consentimento. Será feita posteriormente uma análise detalhada dos direitos dos titulares dos dados.

Será no capítulo quinto que enquadraremos o Regulamento Geral de Protecção de dados com as obrigações dos *Cloud Service Providers*, seja como responsável pelo tratamento dos dados pessoais seja assumindo o papel de subcontratante.

No capitulo sexto, ainda respeitante às obrigações do SCP, serão abordadas temáticas relacionadas com a segurança da informação, fazendo um breve estudo sobre os *Impact Assessments* e as notificações em caso de *Data Breach*.

No capítulo sétimo, será abordada a temática da transferência de dados para países terceiros à União Europeia. Será explicada a Decisão "Porto Seguro" e o Acórdão *Schrems* bem como todo o processo que culminou na invalidade da Decisão. Será ainda abordado o acordo que viria a substituir o "Porto Seguro", tendo sido adoptado pela Comissão um novo quadro transatlântico para os fluxos de dados: o "Escudo de Privacidade" que pretende reflectir os requisitos estabelecidos no Acórdão *Schrems.*

Por último, o capítulo oitavo e final, será dedicado às conclusões retiradas dos problemas abordados e do estudo desenvolvido.

# 2. Enquadramento Histórico

Os conceitos de segurança da informação e protecção de dados tal como os conhecemos hoje diferem em muito do que eram para os nossos antepassados. Podemos considerar que a preocupação de proteger informação remonta às mais antigas trocas de missivas, cartas, bilhetes escoltados por guardas para que chegassem ao destino pretendido intocadas.

Uma forma de assegurar a protecção da informação foi a encriptação, esta data do seculo V a.C., surgindo-nos com os gregos a primeira descrição de um sistema de criptografia militar[5]. A criptanálise terá surgido com os árabes no seculo I d.C. [6] Existem listas dos diversos tipos de criptografia conhecidos na época incluindo sistemas de transposição e substituição.

Na Europa, a criptologia[7] terá começado a desenvolver-se no inicio do século XV em Itália, sendo que o surgimento da diplomacia levou a uma grande evolução da criptografia dado que as embaixadas enviavam regularmente cartas entre si recorrendo à encriptação para tornar essas mensagens indecifráveis.[8]

Foi durante as grandes guerras que se tornou ainda mais notória a evolução da criptografia e o aumento da preocupação dos Estados com a sua informação. Em 1940, durante a Segunda Grande Guerra surge a máquina enigma, utilizada pelos alemães para encriptar as suas comunicações. É então pela mão de Alan Turing[9] que surge o primeiro computador com o objectivo de decifrar as mensagens alemãs.

Durante o início dos anos 70, houve um aumento no uso de computadores e na mesma altura a ARPA (sigla em inglês para Advance Research Projects Agency)

[5] Diz que Júlio César é foi o inventor de um dos mais básicos tipos de cifras de substituição, tendo a cifra o seu nome até aos dias de hoje. A cifra de César codifica uma mensagem deslocando o alfabeto por um número previamente determinado. Substituindo cada letra da mensagem por uma nova.

[6] Encontrat referencia a criptografia militar

[7] Ciência que engloba a criptografia e a criptoanálise.

[8] A Short History of Cryptography, Fred Cohen & Associates, p3 disponível em: http://web.itu.edu.tr/~orssi/dersler/cryptography/Chap2-1.pdf, acedido pela ultima vez e, 4 de Maio de 2018.

[9] A ideia do computador moderno foi-nos introduzida por Alan Turing e por John Von Neumann, com o objetivo comum de conceber uma nova máquina de calcular, que para além dos cálculos conseguiria ter processamento lógico de informações. O primeiro computador operacional foi construído por Alan Turing em 1940, aquando da Segunda Guerra Mundial, com o objetivo de decifrar as mensagens da máquina alemã Enigma.

Agência do Departamento de Defesa Americano, desenvolveria uma pequena rede compreendida por quatro computadores[10], sendo estes os primórdios da internet.[11]

Ainda que a segurança da informação e a protecção de dados seja muito mais abrangente do que a Cibersegurança, é inegável a interligação da evolução tecnológica com a crescente preocupação da protecção de dados.

Aliando a evolução tecnológica desta altura a um aumento do comércio internacional abriram-se novas portas para o processamento de dados a uma escala internacional, e pese embora esses desenvolvimentos tivessem oferecido grandes vantagens no que concerne à eficiência e produtividade, trouxeram consigo uma consciencialização da importância da privacidade dos indivíduos.

## 2.1 Enquadramento Legal

De um ponto de vista legal, o primeiro instrumento a considerar é a Declaração Universal dos Direito Humanos[12] como a base para a protecção dos direitos do indivíduo.

A Declaração dos Direitos Humanos, adoptada pela Assembleia Geral das Nações Unidas no dia 10 de Dezembro de 1948 na "*grande salle*" do Palácio de Chaillot, um teatro em Paris, França, contém disposições específicas relativas ao direito à vida privada e familiar. Os princípios consagrados na Declaração dos Direitos Humanos forneceram, de facto, a base para a maioria das normas ulteriores relativas à protecção de dados.

Pode ler-se no artigo 12º da Declaração, o direito relativo à vida privada, dizendo-nos que *"Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a protecção da lei."*[13]

[10] Em 1982 a ARPAnet, nome dado à rede desenvolvida pela ARPA, juntou-se a outras redes, com o objetivo de fazer transferência de um maior volume de informação. Esta interligação entre várias redes formou uma rede de redes, ou seja, uma Internet.

[11] Vide in POE, T. Marshall, A History of Communications, Cambridge University Press, 2011 – p.213.

[12] A Declaração Universal dos Direitos Humanos foi Adoptada a 10 de Dezembro de 1948 pela Assembleia Geral das Nações Unidas.
Disponível em https://dre.pt/declaracao-universal-dos-direitos-humanos, acedida pela ultima em 7 de Maio de 2018.

[13] Declaração Universal dos Direito Humanos art. 12.

Um outro instrumento de grande relevância foi a Convenção Europeia dos Direitos do Homem[14], assinada em Roma em 1950 e que entrou em vigor dia 3 de Setembro de 1953, aplicando-se apenas aos Estados Membros.

No artigo 8º da Convenção estabelece-se um reconhecimento do direito ao respeito pela vida privada e familiar, pelo domicílio e pela correspondência. Pode ler-se no artigo:

> *"Direito ao respeito pela vida privada e familiar*
> *1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência.*
> *2. Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem - estar económico do país, a defesa da ordem e a prevenção das infracções penais, a protecção da saúde ou da moral, ou a protecção dos direitos e das liberdades de terceiros."*[15]

Do final da década de 1960 até a década de 1980, diversos países, especialmente países Europeus, legislaram sobre o controlo de uso de informações pessoais quer por entidades privadas quer pelo próprio governo.

Em três países europeus, Espanha[16], Portugal e Áustria[17], a protecção de dados também foi incorporada como um direito fundamental na Constituição.

Na constituição da República Portuguesa pode ler-se no artigo 35º sobre a utilização da informática:

> *"1. Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua rectificação e actualização, e o direito de conhecer a finalidade a que se destinam, nos termos previstos na lei.*
> *2. A lei define o conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão*

[14] Convenção Europeia dos Direitos Humanos, dispnivel em https://www.echr.coe.int/Documents/Convention_POR.pdf acedido pela utilma vez a 8 de Maio de 2018.

[15] Convenção Europeia dos Direitos Humanos, Art 8º

[16] Consituição espanhola, artigo 18 "*1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.*
*2.El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.*
*3.Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.*
*4La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos."*

[17] A constituição Austriaca garante a protecção e o respeito pela privacidade no seu artigo 10 fazendo referencia explícita à privacidade das comunicações estabelece que: *"The privacy of letters may not be infringed and the seizure of letters may, except in case of a legal detention or domiciliary visit, take place only in times of war or by reason of a judicial warrant in conformity with existent laws." Article 10A states: "Telecommunications secrecy may not be infringed. Exceptions to the provisions of the foregoing paragraph are admissible only by reason of a judicial warrant in conformity with existent laws.".*

*e utilização, e garante a sua protecção, designadamente através de entidade administrativa independente.*

*3. A informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, a filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis.*

*4. É proibido o acesso a dados pessoais de terceiros, salvo em casos excepcionais previstos na lei.*

*5. É proibida a atribuição de um número nacional único aos cidadãos.*

*6. A todos é garantido livre acesso às redes informáticas de uso público, definindo a lei o regime aplicável aos fluxos de dados transfronteiriços e as formas adequadas de protecção de dados pessoais e de outros cuja salvaguarda se justifique por razões de interesse nacional.*

*7.Os dados pessoais constantes de ficheiros manuais gozam de protecção idêntica à prevista nos números anteriores, nos termos da lei."*[18]

Para evitar uma recolha imprópria de informações pessoais e seguindo a tendência das regulações internas dos países acima mencionados, o Conselho da Europa estabeleceu princípios para a protecção dos dados pessoais, culminando em 1968 com a Recomendação 509[19] sobre Direitos Humanos e Desenvolvimentos Tecnológicos Modernos e Científicos.

Em 1973 e 1974, o Conselho da Europa baseou-se na Recomendação 509 para a elaboração das Resoluções 73/22[20] e 74/29[21], com o objectivo de estabelecer princípios para a protecção de dados pessoais que se encontrassem em bancos de dados automatizados nos sectores público e privado. O objectivo seria promover um padrão para a homogeneidade das legislações nacionais dos Estados Membros.

Tornou-se nesta altura imperativo criar normas internacionais vinculantes de forma a não permitir a divergência de legislações internas que já se fazia notar. É com base neste pensamento que o Conselho da Europa emana, no princípio da década de 80, o primeiro instrumento internacional vinculativo que estabelece padrões para a protecção dos dados pessoais das pessoas: a Convenção para a Protecção das Pessoas relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal[22].

---

[18] Constituição da República Portuguesa, art 35º.

[19] A Declaração Sobre O Uso Do Progresso Científico E Tecnológico Nos Interesses Da Paz E Em Benefício Da Humanidade foi adoptada a 10 de Novembro de 1975 pela Assembleia Geral das Nações Unidas. Disponivel em http://gddc.ministeriopúblico.pt/sites/default/files/decl-progressocientifico.pdf, acedida pela última vez a 10 de Maio de 2018.

[20]Resolution (73) 22 On The Protection Of The Privacy Of Individuals Vis-A-Vis Electronic Data Banks In The Private Sector, adoptada pelo Comite de Ministros a 26 de Setembro de 1973

[21] Resolution (74) 29 On The Protection Of The Privacy Of Individuals Vis-À-Vis Electronic Data Banksin The Public Sector, adoptada pelo Comité de Ministros a 20 de Setembro de 1974.

[22] Convenção para a Protecção das Pessoas Relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal, Conselho da Europa, disponível em

Na Convenção 108, o Conselho da Europa deliberou que as pessoas que tratem informações pessoais em suporte digital têm a responsabilidade de proteger esses dados.

Pode ler-se no preâmbulo da Convenção que esta tem como objectivo alcançar uma maior homogeneidade entre as regulamentações internas dos seus membros, sendo ”desejável alargar a protecção dos direitos e das liberdades fundamentais de todas as pessoas, nomeadamente o direito ao respeito pela vida privada, tendo em consideração o fluxo crescente, através das fronteiras, de dados de carácter pessoal susceptíveis de tratamento automatizado”.[23]

A Convenção 108[24] consiste em três partes principais, a primeira parte contém disposições de direito substantivo na forma de princípios básicos, uma segunda que contém regras especiais sobre fluxos de dados transfronteiriços e uma última parte sobre mecanismos de assistência mútua e consulta entre as partes (Capítulo IV) . No que concerne a fluxos transfronteiriços, relevante para este estudo, pode dizer-se que o Capítulo III da Convenção 108 impõe algumas restrições aos fluxos transfronteiriços de dados pessoais sendo que vai mais além e prevê essas disposições para países onde a lei não oferece protecção.

Pode ler-se no artigo 1º que estabelece os objectivos e finalidades que:

> *“A presente Convenção destina-se a garantir, no território de cada Parte, a todas as pessoas singulares, seja qual for a sua nacionalidade ou residência, o respeito pelos seus direitos e liberdades fundamentais, e especialmente pelo seu direito à vida privada, face ao tratamento automatizado dos dados de carácter pessoal que lhes digam respeito («protecção dos dados»).”*[25]

O número 2 do artigo 12º da Convenção estabelece uma premissa importante no que concerne ao fluxo transfronteiriço, já que no que toca a transferências de informações pessoais entre as partes da convenção, um Estado signatário não poderá “com a exclusiva finalidade de protecção da vida privada, proibir ou submeter a autorização especial os fluxos transfronteiriços de dados de carácter pessoal com destino ao território de uma outra Parte.”[26] A razão desta disposição é a de que os Estados signatários ao concordarem com as disposições de protecção de dados

---

https://www.cnpd.pt/bin/legis/internacional/Convencao108.htm, acedido pela ultima vez a 10 de Julho de 2018.

[23] Convenção para a Protecção das Pessoas Relativamente ao Tratamento Automatizado de Dados(…) art. 1º.

[24] Nome mais comum para a Convenção para a Protecção das Pessoas Relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal.

[25] Convenção para a Protecção das Pessoais Relativamente ao Tratamento Automatizado de Dados (…) op.cit. Artº1.

[26] Convenção para a Protecção das Pessoais Relativamente ao Tratamento Automatizado de Dados (…) op.cit. Art 12º número 2.

mencionadas no Capítulo II, estabelecem entre si o mesmo nível de protecção de dados pessoais. No entanto, no número 3 da mesma norma, há uma ressalva para a derrogação da disposição do número 2. Desta forma afastam-se as disposições no número 2 quando as partes tiverem regras específicas nas suas legislações nacionais para determinadas categorias de dados pessoais, sendo que uma das partes da transacção possa não oferecer o mesmo nível de protecção que a outra, ou ainda quando a transferência se dê de um Estado signatário para um Estado não parte da convenção.[27]

Em 2001 foi aberto para assinatura o Protocolo Adicional à Convenção para a Protecção das Pessoas relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal, respeitante às autoridades de controlo e aos fluxos transfronteiriços de dados[28], entrando em vigor em Julho de 2004 na ordem internacional e em Portugal em 2007. O objectivo da concepção deste protocolo adicional foi estabelecer uma abordagem às medidas que dizem respeito à transferência de informações pessoais para países que não eram signatários da Convenção 108. A solução para tal encontra-se no artigo 2º do protocolo, com a epígrafe "Fluxo transfronteiriço de dados de carácter pessoal para um destinatário que não está sujeito à jurisdição de uma Parte na Convenção", podendo ler-se no texto no artigo:

> *"1 - As Partes deverão prever que a transferência de dados pessoais para um destinatário que esteja sujeito à jurisdição de um Estado ou de uma organização que não seja Parte na Convenção só deve ser efectuada se esse Estado ou essa organização assegurarem um nível de protecção adequado para a transferência pretendida.*
>
> *2 -Por derrogação do disposto no n.º 1 do artigo 2.º do presente Protocolo, uma Parte pode autorizar a transferência de dados pessoais:*
>
> *a) Se o direito interno o previr em virtude de:*
>
> *Interesses específicos da pessoa em causa, ou*
>
> *Interesses legítimos prevalecentes, em especial interesses públicos importantes; ou*
>
> *b) Se a pessoa responsável pela transferência apresentar garantias, nomeadamente aquelas que possam resultar de cláusulas contratuais, e forem julgadas suficientes pelas autoridades competentes, em conformidade com o direito interno."*[29]

Na mesma altura da entrada em vigência da Convenção 108, também a Organização para Cooperação e Desenvolvimento Económico (OCDE) estabeleceu

[27] Convenção para a Protecção das Pessoais Relativamente ao Tratamento Automatizado de Dados (…) op.cit. Art 12º número 3.

[28]Protocolo Adicional À Convenção Para A Protecção Das Pessoas Relativamente Ao Tratamento Automatizado De Dados De Carácter Pessoal, Respeitante Às Autoridades De Controlo E Aos Fluxos Transfronteiriços De Dados disponível em: http://gddc.ministeriopúblico.pt/instrumento/protocolo-adicional-convencao-para-proteccao-das-pessoas-relativamente-ao-tratamento-0, acedido pela ultima vez a 10 de Junho de 2018

[29] Protocolo Adicional À Convenção Para A Protecção(…)op.cit. Art. 2.

directrizes para a Protecção da Privacidade e Fluxos Transfronteiriços de Dados Pessoais, reafirmando mais tarde o seu compromisso para com as Directrizes, em declarações feitas em 1985 e 1998. Nesse documento podem ler-se directrizes a serem seguidas pelo que hoje chamamos de Responsável pelo Tratamento dos Dados, sendo mais relevante ainda para o âmbito desta dissertação as menções das directrizes no que toca à transferência de dados pessoais. Estabelece-se que:

> "Os países Membros deveriam levar em consideração as implicações, para os outros países Membros, do processamento nacional e da reexportação de dados pessoais.
>
> *Os países Membros deveriam tomar todas as disposições razoáveis e adequadas para garantir a continuidade e segurança dos fluxos transfronteiriços de dados pessoais, incluindo durante o trânsito por um país Membro.*
>
> *Um país Membro deveria deixar de restringir os fluxos transfronteiriços de dados entre ele e outro país Membro, salvo se este último ainda não observa substancialmente as Directrizes ou se a reexportação de tais dados escapa à sua legislação doméstica sobre a privacidade. Um país Membro também pode impor restrições relativas a determinadas categorias de dados pessoais para os quais sua legislação doméstica sobre a privacidade inclui regulamentos específicos em função da natureza destes dados, e para os quais um outro país Membro não oferece protecção equivalente"*[30]

Ainda que o objectivo de homogeneizar a legislação interna dos Estados em matéria de protecção de dados tenha de certa forma sido alcançado com a Convenção 108 e as Directrizes da OCDE, estas deixam em aberto como conduzir a implementação das suas normas, e percebeu-se desde logo que tal lacuna poderia ter graves implicações em matéria de direitos fundamentais dos indivíduos.[31]

A Convenção 108 serviu de base à Comissão na elaboração da directiva-quadro, visto que os seus princípios constituíam um conjunto comum de normas para os Estados signatários. A Directiva contemplou estes princípios gerais, estendendo as protecções para dados pessoais automatizados e não automatizados, cobrindo tanto os sectores públicos como privados.

A Directiva 95/46/CE iniciou a sua vigência em Outubro de 1995, sendo estabelecido assim um regime geral de protecção de dados na União Europeia. Este regime não se restringia exclusivamente aos Estados-Membros mas incluía também

[30] Directrizes da OCDE para a Protecção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais pp 5 e 6, disponível em http://www.oecd.org/sti/ieconomy/15590254.pdf acedido pela última vez a 12 de Maio de 2018

[31] Vide JESUS, Ines "O Novo Regime Jurídico de Protecção de Dados Pessoais na Europa", Faculdade de Direito da Universidade Nova de Lisboa 2012. p.2

Estados que, não sendo membros da Comunidade Europeia, pertencessem ao Espaço Económico Europeu.[32]

Com a Directiva estão contemplados critérios como o critério da necessidade, adequação e limitação das finalidades do tratamento, bem como o critério da conservação pelo período necessário para a prossecução das finalidades da recolha.[33]

A Directiva procurou harmonizar as legislações nacionais garantindo, desta forma, um elevado nível de protecção no espaço europeu e promovendo também o mercado único. Ainda assim, e dado que uma Directiva, ao contrário de um regulamento, necessita de uma transposição para a ordem interna, tal levou a que existissem diferenças significativas nas formas como os Estados Membros implementaram e aplicaram a Directiva. Essas inconsistências entre Estados Membros resultaram tanto da aplicação incorrecta da Directiva por parte de alguns Estados como também da implementação da Directiva por cada Estado Membro, fazendo adaptações dentro da margem de manobra permitida. [34]

Quando se aborda o tema do regime jurídico europeu de protecção de dados, é incontornável referir a relevância da Carta dos Direitos Fundamentais da União Europeia, adoptada a 7 Dezembro de 2000 em Nice. [35]

A Carta segue os princípios gerais estabelecidos na Convenção Europeia dos Direitos do Homem, mas contém referências específicas no que concerne à protecção de dados pessoais. Em Dezembro de 2009, quando o Tratado de Lisboa entrou em vigor, a Carta recebeu carácter vinculativo.

O artigo 7º prevê o direito ao respeito pela vida privada e familiar reflectindo o que já se encontrava na CEDH mas é no artigo 8º que encontramos reconhecido o direito à protecção de dados, podendo ler-se:

> *"1. Todas as pessoas têm direito à protecção dos dados de carácter pessoal que lhes digam respeito.*
>
> *2. Esses dados devem ser objecto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva rectificação.*
>
> *3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente."*[36]

[32] Directiva 95/46/CE(…) op.cit.

[33] Directiva 95/46/CE(…)op.cit

[34] Vide, SILVA Heraclides "A Protecção De Dados Pessoais Na Era Global: O Caso Schrems", Faculdade de Direito Universidade Nova de Lisboa 2017.

[35] Carta Dos Direitos Fundamentais Da União Europeia 2012/C 326/02 disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A12012P%2FTXT acedida pela ultima vez a 23 de Julho de 2018.

[36] Carta dos Direitos fundamentais da União Europeia Art8º.

## 2.2 Enquadramento histórico do *cloud computing*

Nas décadas que se seguiram ao aparecimento dos primeiros computadores e das primeiras redes, a computação era, quase na sua totalidade, centralizada. Foi no discurso comemorativo dos 100 anos do MIT que apareceu pela primeira vez o termo *Cloud Computing*. John McCarty foi o primeiro a falar publicamente da ideia, propondo um método chamado de *Time Sharing*, partilhando o poder de processamento de várias máquinas e desta forma potencializando as suas capacidades. Esta ideia, ainda que popular na altura, foi sendo esquecida visto que nem o *hardware* nem o *software* estavam prontos para esta nova era.[37] Apenas na década de 80, com o aparecimento de microprocessadores cada vez melhores e com um custo mais reduzido, computadores pessoais e *workstations* baseados em Unix, se abriu caminho para o novo modelo de computação distribuído baseado em cliente-servidor. A arquitectura desses sistemas cliente-servidor era bem diferente da arquitectura dos *mainframes* do modelo de computação central.

Com o aparecimento da Internet e com a sua posterior privatização em 1991, a Internet deixou de ser do domínio público e passou para a esfera do domínio privado, começando a surgir os primeiros distribuidores de cariz privado de internet, aumentando desta forma o seu crescimento e difusão. Também na mesma década Robert Cailliau, publicava uma proposta para o que viria a ser o que hoje chamamos de *World Wide Web*[38]. Esta rede foi projectada de forma a disponibilizar documentos em hipermédia[39], estando estes conectados entre si e sendo executados através da Internet. Em 1993, o CERN anunciou que a World Wide Web também conhecida por WWW, seria livre para todos, sem custo. A WWW, ainda que não sendo o único serviço disponível na Internet, tornou-se rapidamente o mais popular, em grande parte devido aos protocolos que utiliza, nomeadamente o protocolo de transferência de hipertexto conhecido pelas siglas HTTP, um protocolo da camada de Aplicação do

[37] Vide "História da computação em nuvem: como surgiu a cloud computing?" disponível em https://www.ipm.com.br/blog/historia-da-computacao-em-nuvem-como-surgiu-a-cloud-computing, acedido pela ultima vez 15 de Julho de 2018.

[38] Quanto ao seu funcionamento, visualizar uma página *web* ou outro recurso disponibilizado normalmente inicia-se ou ao digitar uma endereço no navegador ou através de uma hiperligação. Desta forma o protocolo em consonância com um outro protocolo (Domain Name Server) transforma o endereço num IP. O navegador estabelece, então, uma conexão TCP-IP com o servidor *web* localizado no endereço IP retornado o sitio pretendido.

[39] Hipermédia é o termo utilizado para designar a interligação de várias mídias.

modelo de *Open System Interconnection*[40], utilizado para transferência de dados na WWW. Na prática, o que acontece é que o protocolo HTTP faz a comunicação entre o cliente e o servidor através de mensagens. O cliente envia uma mensagem com o objectivo de requisitar um recurso e o servidor envia uma mensagem de resposta ao cliente com a solicitação. Embora nesta altura a maior parte das aplicações assentes na Web seguissem geralmente o modelo cliente-servidor, à medida que a Internet e a *World Wide Web* se foram expandindo e popularizando no mundo, era cada vez mais clara a necessidade de um novo modelo de computação, um modelo baseado na Internet que fosse além dos modelos centralizados e cliente-servidor. O número crescente de utilizadores que acediam a aplicações na Web começava a exigir servidores que fossem cada vez mais escalonáveis. Desta forma muitos servidores Web começaram a ser hospedados em *data-centers*. Vários factores, nomeadamente a capacidade de partilhar trabalho e a oferta de ferramentas sofisticadas de gestão de sistemas, fizeram com que houvesse uma grande migração de serviços para esse modelo.[41]

É assim nesta altura que o modelo *Cloud* volta a ser equacionado, inicialmente ligado ao mobile. Com o passar do tempo e a constante inovação, começam a surgir os primeiros serviços de *"Software as a Service*". Um desses primeiros projectos é o SalesForce.com, que desenvolveu um modelo de negócio baseado nos serviços on-*demand*. A partir dos anos 2000, conscientes da importância deste fenómeno, a Microsoft e a IBM começam a trabalhar nos seus próprios serviços *Cloud* e em 2005 a Amazon lança a *Amazon Web Service*, onde adequa os seus *data-centers* a esta nova realidade. Nos anos que se seguiram tanto a Google como a *Microsoft* desenvolveram as suas próprias ferramentas.

# 3.Enquadramento Tecnológico

## 3.1 Conceito de *cloud*

De uma forma simples e do ponto de vista do utilizador a computação em nuvem oferece uma forma simples de aceder a servidores, armazenamento, bancos de informação entre outros serviços através da Internet. Na verdade não existe um

[40] O modelo Open System Interconnection, conhecido por modelo OSI é a par do modelo de TCP/IP um modelo de camadas, com objetivo de estabelecer uma padronização, para protocolos de comunicação .
[41]Vide FOOTE, Keith D. "A Brief History of Cloud Computing", disponível em http://www.dataversity.net/brief-history-cloud-computing/ acedido pela ultima vez a 27 de Junho de 2018

conceito completamente novo quando nos referimos à *Cloud*, dado que tecnologias que dela fazem parte já existiam, o que acontece é que há uma integração de tecnologias já existentes, que juntas dão origem à computação em *cloud*.[42]

A *cloud* é formada por três componentes: *storage, nodes* e um controlador. Segundo o NIST, a *cloud* é "um modelo que viabiliza convenientemente, *on-demand network* a um conjunto partilhado de recursos computacionais configuráveis (por exemplo, redes, servidores, armazenamento, aplicações e serviços) que podem ser rapidamente facultados com o mínimo esforço de gestão ou intervenção dos prestadores do serviço."[43] No entanto, a verdade é que esta temática sempre gerou controvérsia na comunidade, o problema reside no facto de tantas empresas usarem a nuvem com objectivos e de formas distintas. Assim, é visto que qualquer forma de computação acessível através de uma rede e quase todo tipo de actividade que envolve acesso a conjuntos de dados em massa, caem no escopo do *cloud computing*.[44]

Desta forma, para alguns, a *cloud* diz respeito a pesquisas na web, para outros diz respeito a redes sociais, enquanto que outros ainda pensam na nuvem como uma tecnologia de *outsourcing,* permitindo enviar dados para algum lugar remoto onde computação e armazenamento são baratos. Todas essas visões são absolutamente corretas. [45]

Muitas foram também as definições que foram dadas à computação em *cloud*. A IBM descreve como "*Cloud computing, often referred to as simply "the cloud," is the delivery of on-demand computing resources — everything from applications to data centers — over the internet on a pay-for-use basis."*[46] Enquanto isso a Amazon descreve o modelo como "a entrega sob demanda de poder computacional, armazenamento de banco de dados, aplicações e outros recursos de TI por meio de uma plataforma de serviços de nuvem via Internet com uma definição de preço conforme o uso."[47]

[42]Vide FOOTE, Keith D. A Brief History of Cloud (…) op.cit.

[43] Vide in "The NIST Definition of Cloud Computing" p.2

[44] Vide in MELL PeteR, GRANCE Timothy . "The NIST Definition of Cloud Computing" p.2

[45] FOOTE, Keith D. "A Brief History of Cloud (…)"

[46] IBM, "what is Cloud Computing" disponivel em a https://www.ibm.com/cloud/learn/what-is-cloud-computing, acedido pela ultima vez a 05 de Junho de 2018.

[47] Amazon "o que é o cloud Computing" disponivel em https://aws.amazon.com/pt/what-is-cloud-computing/ acedido pela ultima vez a 10 de Junho.

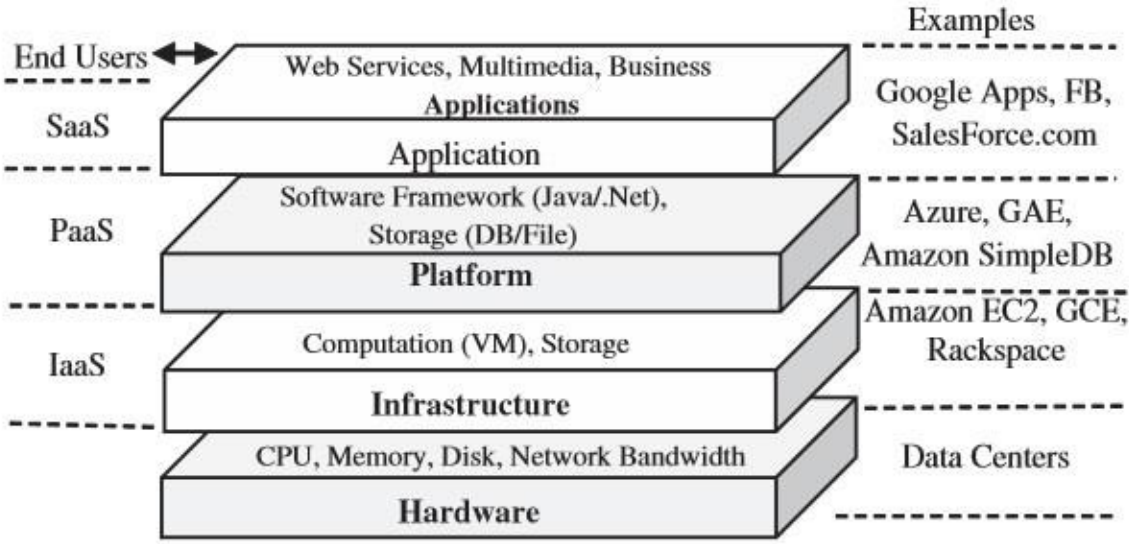


Imagem 3.1: Arquitectura de *Cloud Computing*

## 3.2 Modelos de serviço de *Cloud Computing*

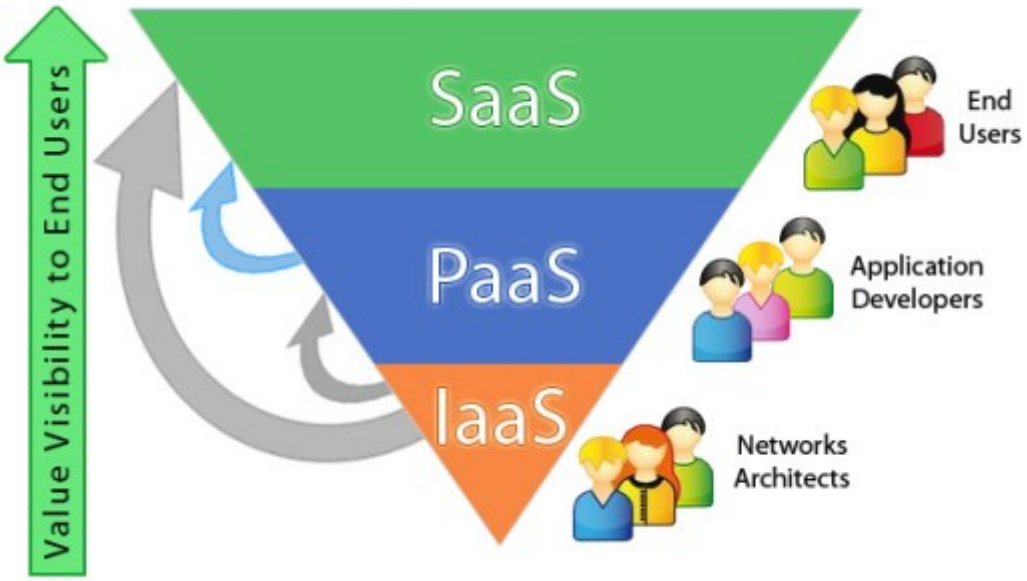


Imagem 3.2: Os três modelos de *Cloud*

### 3.2.1 A *Cloud* como *Infrastructure* as a *service*

IaaS é o acrónimo de *infraestruture as a service* . Através deste sistema o utilizador tem à sua disposição todos recursos computacionais de infra-estrutura, sem ter que se preocupar com o hardware ou com a continuidade do serviço em caso de falha, pois cabe ao prestador de serviço lidar com esses aspectos de mais baixo nível. [48]

Os recursos podem ser por exemplo, recursos de rede, servidores, espaço de armazenamento entre outros.

### 3.2.2 A *Cloud* como *Platform* as a *service*

PaaS é o acrónimo de *plataform as a service*. Aqui não está subjacente a questão da infra-estrutura na qual assenta a plataforma, já que essa preocupação caberá a quem oferece o serviço de IaaS. Na pratica é disponibilizada uma plataforma para que a entidade possa desenvolver e gerir o seu *sofwar*e. Neste caso, existem menos encargos, mas também uma menor flexibilidade. [49]

A baixa portabilidade é uma grande desvantagem, por exemplo no caso de *SalesForce*, devido à sua base de dados e linguagem de programação de "código fechado", apenas se pode desenvolver uma aplicação utilizando a linguagem de programação Apex[50], sendo que só poderá ser executada na Infra-estrutura *cloud* da SalesForce.com.[51]

### 3.2.3 A *Cloud* como *Software as a service*

SaaS é o acrónimo de *Software as a Service*, usado frequentemente para identificar uma aplicação de software que funciona na *cloud*. Trata-se de um modelo de distribuição de software que permite o uso de aplicações exclusivamente por meio

[48] Vide KAI Hwang, GEOFFREY Fox, DONGARRA Jack, "Distribuited and Cloud Computing: from Parallel Processomg to the Internet of Things", Elsevier , 2012 p. 200

[49] Vide KAI Hwang, GEOFFREY Fox, DONGARRA Jack, "Distribuited and Cloud Computing (…)op.cit. p. 203

[50] A salesforce.com deu origem `Q primeira linguagem de programação para cloud computinga Apex. A Apex é semelhante à linguagem Java, e é a mais popular para aplicações Web e funciona nos servidores da plataforma Force.com.

[51] Vide KAI Hwang, GEOFFREY Fox, DONGARRA Jack, "Distribuited and Cloud Computing (…)op.cit. p. 203

de um browser[52]. Desta forma o utilizador tem conhecimento de onde o software está hospedado, em que sistema operacional é executado e em que linguagem de programação foi desenvolvido. Localmente não existe a necessidade de qualquer instalação, sendo que apenas é necessário um qualquer browser. Exemplos de SaaS são o serviços de email , CRM (Client Relationship Management) ou os serviços de armazenamento como o OneDrive DropBox e GoogleDrive.[53]

Esse tipo de serviço é normalmente facturado periodicamente com base no número de utilizadores activos.

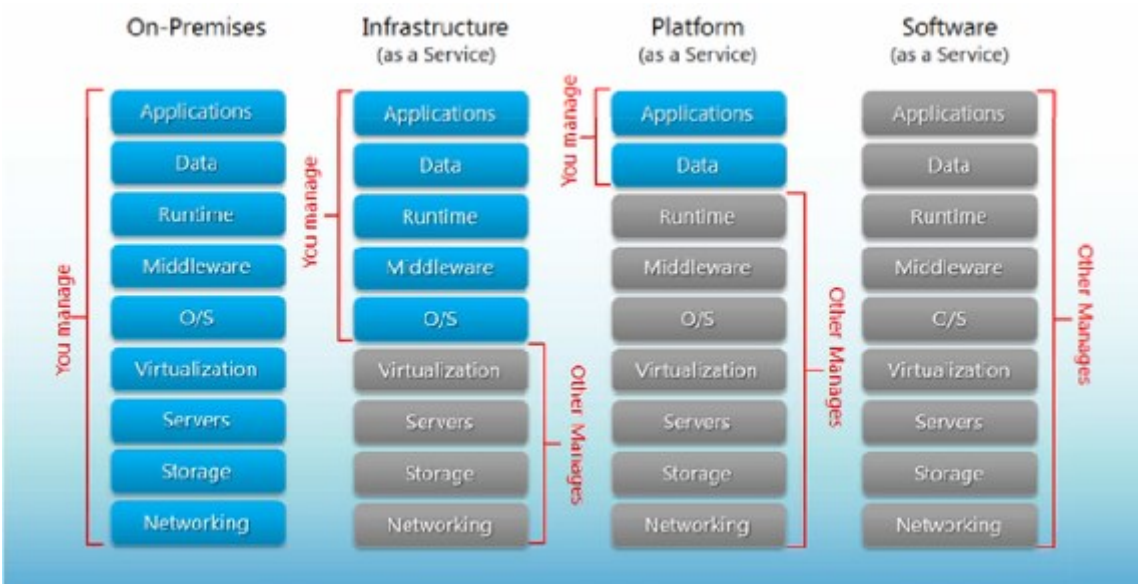


**Imagem 3.3: Responsabilidade nas três arquitecturas da *cloud***

## 3.4 Modelos de Desenvolvimento

### 3.4.1 *Cloud* Privada

A *cloud* privada, também chamada de *cloud* interna, trata-se de uma infra-estrutura desenvolvida e gerida de forma exclusiva para uma entidade ou grupo de entidades. Este tipo de *cloud* poderá ser de propriedade interna ou funcionar com um modelo de *leasing*. Consoante seja interna ou em *leasing*, no que concerne à sua localização esta

[52] KAI Hwang, GEOFFREY Fox, DONGARRA Jack, "Distribuited and Cloud Computing(…)"p. 203.

[53] BUYYA, BRIBERG, GOSCINKI " *Cloud computing : principles and paradigms"* , John Wiley & Sons, Inc 2011 p.15

poderá estar alojada internamente ou hospedada no exterior numa infra-estrutura de terceiros. Este modelo garante ao proprietário da *cloud* uma maior segurança e controlo dos recursos e clientes da infra-estrutura. O NIST descreve-nos a *cloud* privada "como uma infra-estrutura em que a operação é direccionada apenas para um cliente *cloud*, com a gestão efectuada pelo próprio ou por uma terceira entidade, e que, normalmente, a infra-estrutura de suporte se encontra dentro da propriedade do cliente."[54]

Relativamente a custos, dado que a organização adquire e gere toda a infra-estrutura, este modelo será assim mais oneroso que outros modelos, nomeadamente que o modelo de *cloud* pública.

Exemplos de *cloud* privada são a *VMWare* e a *SalesForce*.

### 3.4.2 *Cloud* Pública

A *cloud* pública também chamada de *cloud* externa, trata-se de um recurso disponibilizado por um *cloud provider*. Neste modelo a propriedade da infra-estruta de *cloud* é de uma organização que a disponibiliza ou vende ao público em geral ou a uma empresa. Este é o modelo mais utilizado, encontrando-se disponível através de um acesso à internet. Diferentemente da *cloud* privada, a gestão de risco da infra-estrutura não caberá à entidade que está a utilizar a *cloud* mas sim ao *Cloud Provider*, no entanto as garantias de segurança e privacidade dos dados são também menores, o facto de ser o fornecedor a gerir a infra-estrutura retira ao cliente o controlo e gestão da segurança física e lógica da infra-estrutura.[55]

O NIST descreve este modelo de *cloud* como "uma infra-estrutura localizada dentro da propriedade do fornecedor que é aprovisionada para uso aberto ao público em geral, podendo a propriedade, a gestão e a operação ser efectuada por organizações de âmbito empresarial, académico ou governamental."[56]

Exemplos de *cloud* pública são *a Amazon Elastic Compute Cloud, Blue Cloud IBM, Sun Cloud, Google App Engine* e *Windows Azurre Services Platform*.

Os custos deste modelo de *cloud* são menores comparativamente com a *cloud* privada.

---

[54] Vide in MELL Peter, GRANCE Timothy . "The NIST Definition of Cloud Computing" p.7
[55] BUYYA, BRIBERG, GOSCINKI " *Cloud computing : principles and paradigms"* , John Wiley & Sons, Inc 2011 p.15
[56] Vide in MELL Peter, GRANCE Timothy . "The NIST Definition of (..)"op.cit. p.7

### *3.4.3 Cloud* Comunitária

Tal como o nome faz deduzir neste modelo existe aqui uma partilha de infra-estrutura e recursos, poder-se-á dizer que este modelo se pode colocar entre o modelo de *cloud* pública e o modelo de *cloud* privada. O NIST define este modelo como " uma *cloud* comunitária é uma infra-estrutura partilhada por várias organizações, pertencendo a uma comunidade específica e partilhando objectivos comuns, como a missão, os requisitos de segurança e as políticas e considerações de conformidade. A gestão pode ser efectuada pelas organizações ou por terceiros e a sua localização ser interna ou externa. "[57]

### 3.4.4 *Cloud* Híbrida

Como o nome faz transparecer, este tipo de *cloud* é formada pela combinação de outros modelos, como público, privado ou comunitário.

O NIST descreve este modelo como "uma combinação de dois ou dos três modelos (Pública, Privada e Comunitária), os quais continuam a existir isoladamente, mas são integrados por meio de tecnologia proprietária ou aberta, que viabiliza a portabilidade e mobilidade da informação e aplicações."[58]

O objectivo deste modelo é reduzir as desvantagem dos modelos descritos anteriormente, tendo um produto mais flexível, que permite recorrer a *cloud* privada para informações ou dados mais sensíveis e a uma *cloud* pública para dados de cariz menos sensível.[59]

[57] Vide MELL Peter, GRANCE Timothy . "The NIST Definition of Cloud Computing" p.7
[58] Vide MELL Peter, GRANCE Timothy . "The NIST Definition of (…)"op.cit. p.7
[59]Vide BUYYA, BRIBERG, GOSCINKI " *Cloud computing : principles and paradigms"* , John Wiley & Sons, Inc 2011

# 4. Protecção de dados: o Regulamento Geral de Protecção de Dados

Ainda que existam normas internas de outros Estados é para nós neste estudo relevante o diploma que vigora na União Europeia.

O regulamento geral para a protecção de dados pessoais (UE) 2016/679 do Parlamento Europeu e do Conselho (Regulamento Geral de Protecção de Dados ou RGPD), doravante designado apenas por regulamento, é a legislação europeia de protecção de dados. O regulamento data de 27 de Abril de 2016, passando a ter sido aplicado directamente a partir de 25 de maio de 2018.

O Regulamento é aplicado aos 28 Estados Membros, e por não carecer de transposição para a ordem interna de cada Estado, leva a uma harmonização da protecção de dados na União Europeia.

O Regulamento vem revogar a Directiva 95/46/CE e com este nascem também novos direitos para os titulares dos dados, como o direito à portabilidade dos dados, o direito ao esquecimento e o direito de oposição, que serão abordados mais à frente. Vem também trazer algumas alterações no que toca aos responsáveis pelo tratamento dos dados e subcontratantes, particularmente relevante na temática da *cloud*.

No que toca ao âmbito de aplicação, este regulamento é bastante amplo visto que é aplicável a tratamento de dados de titulares de dados pessoais Europeus, ou seja, o responsável pelo tratamento poder-se-á ou não encontrar na União. Sendo esta particularidade relevante para esta dissertação, dado que muitos *providers* de serviços *cloud* não se encontram na UE. O artigo 3º no que concerne ao âmbito territorial de aplicação diz-nos que :

> *"1. O presente regulamento aplica-se ao tratamento de dados pessoais efectuado no contexto das actividades de um estabelecimento de um responsável pelo tratamento ou de um subcontratante situado no território da União, independentemente de o tratamento ocorrer dentro ou fora da União.*
>
> *2. O presente regulamento aplica-se ao tratamento de dados pessoais de titulares residentes no território da União, efectuado por um responsável pelo tratamento ou subcontratante não estabelecido na União, quando as actividades de tratamento estejam relacionadas com:*
>
> *a) A oferta de bens ou serviços a esses titulares de dados na União, independentemente da exigência de os titulares dos dados procederem a um pagamento;*
>
> *b) O controlo do seu comportamento, desde que esse comportamento tenha lugar na União.*

*3. O presente regulamento aplica-se ao tratamento de dados pessoais por um responsável pelo tratamento estabelecido não na União, mas num lugar em que se aplique o direito de um Estado-Membro por força do direito internacional público."*[60]

## 4.1 Definição de Dados Pessoais e Categoria Especial de Dados

No que concerne à definição de dados pessoais, o Regulamento Geral no número 1 do seu artigo 4º define-nos dado pessoal como a "informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, directa ou indirectamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via electrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular"[61].

No âmbito nacional também a Constituição da República Portuguesa contempla nos artigos 26º e 35º, o direito à vida privada e a protecção dos dados pessoais de cada ser humano. O artigo 26º dispõe que "A todos são reconhecidos os direitos à identidade pessoal, ao desenvolvimento da personalidade, à capacidade civil, à cidadania, ao bom nome e reputação, à imagem, à palavra, à reserva da intimidade da vida privada e familiar e à protecção legal contra quaisquer formas de discriminação."[62] Já o artigo 35º da CRP, como vimos anteriormente diz respeito à utilização da Informática.

No que concerne à categoria especial de dados, diz-nos o artigo 9º do regulamento, com a epígrafe, "tratamento de categorias especiais de dados pessoais" que se consideram dados pertencentes a uma categoria especial "dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa".[63]

[60] Regulamento Geral de Protecção (…)op.cit. Art. 3º.
[61] Regulamento Geral de Protecção (…) op.cit.Art. nº4
[62] Constiuição da República Portuguesa Art. 26º.
[63]Regulamento Geral de Protecção (…). op.cit.Art. 9º.

No entanto várias são as excepções ao número 1 deste artigo, encontrando-se estas elencandas no número 2:

> *"2. O disposto no n.o 1 não se aplica se se verificar um dos seguintes casos:*
>
> *a) Se o titular dos dados tiver dado o seu consentimento explícito para o tratamento desses dados pessoais para uma ou mais finalidades específicas, excepto se o direito da União ou de um Estado-Membro previr que a proibição a que se refere o n.o 1 não pode ser anulada pelo titular dos dados;*
>
> *b) Se o tratamento for necessário para efeitos do cumprimento de obrigações e do exercício de direitos específicos do responsável pelo tratamento ou do titular dos dados em matéria de legislação laboral, de segurança social e de protecção social, na medida em que esse tratamento seja permitido pelo direito da União ou dos Estados-Membros ou ainda por uma convenção colectiva nos termos do direito dos Estados-Membros que preveja garantias adequadas dos direitos fundamentais e dos interesses do titular dos dados;*
>
> *c) Se o tratamento for necessário para proteger os interesses vitais do titular dos dados ou de outra pessoa singular, no caso de o titular dos dados estar física ou legalmente incapacitado de dar o seu consentimento;*
>
> *d) Se o tratamento for efectuado, no âmbito das suas actividades legítimas e mediante garantias adequadas, por uma fundação, associação ou qualquer outro organismo sem fins lucrativos e que prossiga fins políticos, filosóficos, religiosos ou sindicais, e desde que esse tratamento se refira exclusivamente aos membros ou antigos membros desse organismo ou a pessoas que com ele tenham mantido contactos regulares relacionados com os seus objetivos, e que os dados pessoais não sejam divulgados a terceiros sem o consentimento dos seus titulares;*
>
> *e) Se o tratamento se referir a dados pessoais que tenham sido manifestamente tornados públicos pelo seu titular;*
>
> *f) Se o tratamento for necessário à declaração, ao exercício ou à defesa de um direito num processo judicial ou sempre que os tribunais atuem no exercício da sua função jurisdicional;*
>
> *g) Se o tratamento for necessário por motivos de interesse público importante, com base no direito da União ou de um Estado-Membro, que deve ser proporcional ao objectivo visado, respeitar a essência do direito à protecção dos dados pessoais e prever medidas adequadas e específicas que salvaguardem os direitos fundamentais e os interesses do titular dos dados;*
>
> *h) Se o tratamento for necessário para efeitos de medicina preventiva ou do trabalho, para a avaliação da capacidade de trabalho do empregado, o diagnóstico médico, a prestação de cuidados ou tratamentos de saúde ou de acção social ou a gestão de sistemas e serviços de saúde ou de acção social com base no direito da União ou dos Estados-Membros ou por força de um contrato com um profissional de saúde, sob reserva das condições e garantias previstas no nº3;*
>
> *i) Se o tratamento for necessário por motivos de interesse público no domínio da saúde pública, tais como a protecção contra ameaças transfronteiriças graves para a saúde ou para assegurar um elevado nível de qualidade e de segurança dos cuidados de saúde e dos*

*medicamentos ou dispositivos médicos, com base no direito da União ou dos Estados Membros que preveja medidas adequadas e específicas que salvaguardem os direitos e liberdades do titular dos dados, em particular o sigilo profissional;*

*j) Se o tratamento for necessário para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos, em conformidade com o artigo 89.o, n.o 1, com base no direito da União ou de um Estado-Membro, que deve ser proporcional ao objectivo visado, respeitar a essência do direito à protecção dos dados pessoais e prever medidas adequadas e específicas para a defesa dos direitos fundamentais e dos interesses do titular dos dados.*

*3. Os dados pessoais referidos no n.o 1 podem ser tratados para os fins referidos no n.o 2, alínea h), se os dados forem tratados por ou sob a responsabilidade de um profissional sujeito à obrigação de sigilo profissional, nos termos do direito da União ou dos Estados-Membros ou de regulamentação estabelecida pelas autoridades nacionais competentes, ou por outra pessoa igualmente sujeita a uma obrigação de confidencialidade ao abrigo do direito da União ou dos Estados-Membros ou de regulamentação estabelecida pelas autoridades nacionais competentes."*[64]

Desta forma e como descrito no artigo apenas será lícito o tratamento destes dados pessoais depois de passar aos filtros do número 2 e 3 do artigo acima mencionado.

## 4.2 Conceito de tratamento

Na definição que nos dá o regulamento no número 2 do artigo 4º o tratamento é " uma operação ou um conjunto de operações efectuadas sobre os dados pessoais ou sobre conjunto de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição".[65]

No entanto, para que haja um tratamento lícito desses dados é necessário que o titular dos dados conceda uma autorização para esse tratamento, ou seja que dê o consentimento, sendo que este deverá ser expresso e obtido de forma lícita.

Para além do regulamento, no âmbito do Direito interno, a Constituição da República no seu artigo 35º "Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua rectificação e actualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei." [66]

[64] Regulamento Geral de Protecção (…)op.cit.Nº 2 Art. 9º.
[65] Regulamento Geral de Protecção (…)op.cit.Nº 2 Art. 4º.
[66] Constituição da República Portuguesa Art. 35º.

## 4.3 O consentimento

Analisando a Carta dos Direitos Fundamentais, no seu artigo 8º é clara uma abordagem ao consentimento, sendo que no seu artigo 8º pode ler-se:

> *"1. Toda a pessoa tem direito à protecção dos dados pessoais que lhe digam respeito;*
> *2. Esses dados devem ser tratados leal, para fins específicos e com base no consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Toda pessoa tem direito de acesso aos dados coligidos que lhes digam respeito e o direito de ter a respectiva rectificação;*
> *3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente".* [67]

Na análise deste artigo da CDF concluímos que o consentimento da pessoa interessada serve de base ao tratamento legítimo dos seus dados pessoais. Desta forma, acreditamos que o consentimento é um pilar fundamental no que concerne à protecção de dados.

O Regulamento Geral de Protecção de dados dá-nos no número 11 do artigo 4º uma definição de consentimento, dizendo-nos que o Consentimento do titular de dados é "uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular de dados aceita, mediante declaração ou acto positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objecto de tratamento".[68]

Diferentemente do que acontecia antes da entrada em vigor do novo regulamento, o consentimento deixou de poder ser dado tacitamente. Existe agora a obrigatoriedade deste ser dado de forma explícita através de um acto positivo. O considerando 32 do regulamento dá-nos indicações das formas de consentimento, podendo este ter a forma oral, escrita ou até revestir forma electrónica " *O consentimento pode ser dado validando uma opção ao visitar um sítio web na Internet, seleccionando os parâmetros técnicos para os serviços da sociedade da informação ou mediante outra declaração ou conduta que indique claramente nesse contexto que aceita o tratamento proposto dos seus dados pessoais. O silêncio, as opções pré-validadas ou a omissão não deverão, por conseguinte, constituir um consentimento."*[69]

O consentimento, segundo o artigo 7º é apenas uma das formas que possibilitam a execução do tratamento dos dados. Acreditamos que esta validação reveste aqui um carácter subsidiário das outras formas de tratamento lícito, visto que na ausência de

[67] Carta dos Direitos Fundamentais Art. 8º
[68] Regulamento Geral de Protecção (…). op.cit.Art. 4º nº 11
[69] Regulamento Geral de Protecção (…). op.cit. Considerando nº 32.

qualquer uma das outras possibilidades o consentimento validará sempre o tratamento dos dados.

Segundo o considerando número 46 do regulamento, ainda que não haja consentimento ou o tratamento não se puder basear noutro fundamento jurídico, o tratamento é considerado lícito quando for necessário à protecção de um interesse essencial à vida do titular dos dados.[70]

## 4.4 Direitos dos Titulares dos dados

Com o novo regulamento foram vários os direitos que nos foram introduzidos ou reformulados. Serão abordados aqui Direitos dos titulares dos dados como o direito a ser informado da localização dos dados de forma a poder exercer os direitos como de acesso, rectificação, apagamento, portabilidade e ou oposição.

### 4.4.1 Direito da transparência

O Direito à transparência é aqui, mais do que tudo, o direito a ser informado das regras para o exercício de todos os outros direitos a quem dispõe. Essa informação deverá ser transmitida utilizando uma linguagem clara e simples, dando especial ênfase à comunicação com crianças.[71]

O responsável pelo tratamento dos dados, para além de informar e facilitar o exercício dos direitos do titular, deve ainda dar seguimento a pedidos dos titulares dos dados no que concerne aos direitos elencados do artigo 15º ao artigo 22º.

O Direito à transparência encontra-se previsto no artigo 12º do regulamento.

### 4.4.2 Direito à Informação

O Direito à informação assenta na informação que deve ser prestada ao titular dos dados, no que concerne ao RGPD este Direito está contemplado nos artigos 13º e 14º, onde são nominadas as informações a facultar ao titular. As informações a serem facultadas vão depender se os dados forem recolhidos junto ou não do titular. Segundo o *artigo 13º do RGPD com a epígrafe "Informação a facultar quando os dados pessoais são recolhidos junto do titular"*

[70] Regulamento Geral de Protecção (…) op.cit. Considerando nº 46.
[71] Regulamento Geral de Protecção (…) op.cit..Art.12

*"1. Quando os dados pessoais forem recolhidos junto do titular, o responsável pelo tratamento faculta-lhe, aquando da recolha desses dados pessoais, as seguintes informações:*

*a) A identidade e os contactos do responsável pelo tratamento e, se for caso disso, do seu representante;*

*b) Os contactos do encarregado da protecção de dados, se for caso disso;*

*c) As finalidades do tratamento a que os dados pessoais se destinam, bem como o fundamento jurídico para o tratamento;*

*d) Se o tratamento dos dados se basear no artigo 6.o, n.o 1, alínea f), os interesses legítimos do responsável pelo tratamento ou de um terceiro;*

*e) Os destinatários ou categorias de destinatários dos dados pessoais, se os houver;*

*f) Se for caso disso, o facto de o responsável pelo tratamento tencionar transferir dados pessoais para um país terceiro ou uma organização internacional, e a existência ou não de uma decisão de adequação adoptada pela Comissão ou, no caso das transferências mencionadas nos artigos 46.o ou 47.o, ou no artigo 49.o, n.o 1, segundo parágrafo, a referência às garantias apropriadas ou adequadas e aos meios de obter cópia das mesmas, ou onde foram disponibilizadas.*

*2. Para além das informações referidas no n.o 1, aquando da recolha dos dados pessoais, o responsável pelo tratamento fornece ao titular as seguintes informações adicionais, necessárias para garantir um tratamento equitativo e transparente:*

*a) Prazo de conservação dos dados pessoais ou, se não for possível, os critérios usados para definir esse prazo;*

*b) A existência do direito de solicitar ao responsável pelo tratamento acesso aos dados pessoais que lhe digam respeito, bem como a sua rectificação ou o seu apagamento, e a limitação do tratamento no que disser respeito ao titular dos dados, ou do direito de se opor ao tratamento, bem como do direito à portabilidade dos dados;*

*c) Se o tratamento dos dados se basear no artigo 6.o, n.o 1, alínea a), ou no artigo 9.o, n.o 2, alínea a), a existência do direito de retirar consentimento em qualquer altura, sem comprometer a licitude do tratamento efectuado com base no consentimento previamente dado;*

*d) O direito de apresentar reclamação a uma autoridade de controlo;*

*e) Se a comunicação de dados pessoais constitui ou não uma obrigação legal ou contratual, ou um requisito necessário para celebrar um contrato, bem como se o titular está obrigado a fornecer os dados pessoais e as eventuais consequências de não fornecer esses dados;*

*f) A existência de decisões automatizadas, incluindo a definição de perfis, referida no artigo 22.o, n.os 1 e 4, e, pelo menos nesses casos, informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados.*

*3. Quando o responsável pelo tratamento dos dados pessoais tiver a intenção de proceder ao tratamento posterior dos dados pessoais para um fim que não seja aquele para o qual os dados tenham sido recolhidos, antes desse tratamento o responsável fornece ao titular dos dados informações sobre esse fim e quaisquer outras informações pertinentes, nos termos do n.o 2.*

*4. Os n.os 1, 2 e 3 não se aplicam quando e na medida em que o titular dos dados já tiver conhecimento das informações."*[72]

No que diz respeito às informações prestadas se os dados não forem recolhidos junto do titular, estas estão previstas no artigo 14º do RGPD que difere do artigo 13º no número 2 e 3, sendo que acresce ao responsável pelo tratamento a responsabilidade de facultar as seguintes informações:

"2 f)A origem dos dados pessoais e, eventualmente, se provêm de fontes acessíveis ao público;

3. O responsável pelo tratamento comunica as informações referidas nos n.os 1 e 2:

a) Num prazo razoável após a obtenção dos dados pessoais, mas o mais tardar no prazo de um mês, tendo em conta as circunstâncias específicas em que estes forem tratados;

b) Se os dados pessoais se destinarem a ser utilizados para fins de comunicação com o titular dos dados, o mais tardar no momento da primeira comunicação ao titular dos dados; ou

c) Se estiver prevista a divulgação dos dados pessoais a outro destinatário, o mais tardar aquando da primeira divulgação desses dados."[73]

Claro está que estas informações não são necessárias caso se comprove que o titular dos dados já tenha conhecimento destas ou caso se comprove que existe uma "impossibilidade de disponibilizar a informação, ou que o esforço envolvido seja desproporcionado"[74], ou ainda caso os dados pessoais sejam confidenciais em virtude de sigilo profissional ou regulamentação interna ou da UE.

### 4.4.3 Direito de acesso do titular dos dados

O Direito de acesso, assenta no direito que o titular dos dados tem de obter a informação, sabendo se os seus dados estão ou não a ser alvo de tratamento e poder ter acesso a esses dados. Segundo o número 3 do artigo 15º, para esse direito ser cumprido, o responsável do tratamento terá de disponibilizar ao titular *"uma cópia dos dados pessoais em fase de tratamento*"[75] , podendo esta cópia revestir forma física ou electrónica, sendo que o responsável poderá exigir o pagamento de uma taxa relativa

[72] Regulamento Geral de Protecção (…)op.cit.Art 13º.
[73] Regulamento Geral de Protecção (…)op.cit.Art.14º.
[74] Regulamento Geral de Protecção (…). op.cit.Art.14º.
[75] Regulamento Geral de Protecção (…). op.cit.Art.15º.

a custos administrativos. O Direito de acesso esta previsto no artigo 15º do regulamento, podendo ler-se:

> *"1. O titular dos dados(…) tem o direito de aceder aos seus dados pessoais e às seguintes informações:*
> *a) As finalidades do tratamento dos dados;*
> *b) As categorias dos dados pessoais em questão;*
> *c) Os destinatários ou categorias de destinatários a quem os dados pessoais foram ou serão divulgados, nomeadamente os destinatários estabelecidos em países terceiros ou pertencentes a organizações internacionais;*
> *d) Se for possível, o prazo previsto de conservação dos dados pessoais, ou, se não for possível, os critérios usados para fixar esse prazo;*
> *e) A existência do direito de solicitar ao responsável pelo tratamento a rectificação, o apagamento ou a limitação do tratamento dos dados pessoais no que diz respeito ao titular dos dados, ou do direito de se opor a esse tratamento;*
> *f) O direito de apresentar reclamação a uma autoridade de controlo;*
> *g) Se os dados não tiverem sido recolhidos junto do titular, as informações disponíveis sobre a origem desses dados;*
> *h) A existência de decisões automatizadas, incluindo a definição de perfis, referida no artigo 22.o, n.os 1 e 4, e, pelo menos nesses casos, informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados.*
> *2. Quando os dados pessoais forem transferidos para um país terceiro ou uma organização internacional, o titular dos dados tem o direito de ser informado das garantias adequadas, nos termos do artigo 46.o relativo à transferência de dados. (…)"*[76]

### 4.4.4 Direito à Rectificação

O direito à rectificação diz respeito ao direito que o titular dos dados tem em rectificar os seus dados, ou seja, dados que estejam desactualizados, incompletos ou até mesmo dados que não sejam correctos. O artigo 16º do RGPD estabelece que "o titular tem o direito de obter (…) do responsável pelo tratamento a rectificação dos dados pessoais inexactos que lhe digam respeito. Tendo em conta as finalidades do tratamento, o titular dos dados tem direito a que os seus dados pessoais incompletos sejam completados, incluindo por meio de uma declaração adicional."[77]

[76] Regulamento Geral de Protecção (…)op.cit.Art.15.
[77] Regulamento Geral de Protecção (…)op.cit.Art.16º.

### 4.4.5 Direito ao esquecimento

O termo direito ao esquecimento tem origem no Direito Francês vinda da expressão "le droit à l'oubli". No ordenamento jurídico francês trata-se do direito pelo qual um indivíduo que cumpriu pena criminal pode opor-se à públicação dos factos da sua condenação depois de ter cumprido a pena. [78]

Em 2012, a vice-presidente da Comissão Europeia Viviane Reding, Comissária europeia responsável pela Justiça, Direitos Fundamentais e Cidadania, propôs ao Parlamento Europeu regulamentar o direito ao esquecimento dizendo que é "importante dar às pessoas o controle sobre os seus dados: o direito de ser esquecido...as pessoas terão o direito - e não apenas a "possibilidade" - de retirar o seu consentimento para o tratamento dos dados pessoais que deram por si próprios" acrescentando que "A Internet tem uma capacidade de procura e memória quase ilimitada. Portanto, mesmo minúsculos restos de informações pessoais podem ter um enorme impacto... O direito de ser esquecido irá basear-se em regras já existentes para lidar melhor com os riscos de privacidade on-line. É o indivíduo que deve estar na melhor posição para proteger a privacidade de seus dados, escolhendo se deve ou não fornecê-los".[79] Assim, em 2012 a Comissão Europeia dá início a trabalhos de revisão legislativa, incluindo nessa revisão um regulamento para Protecção de Dados Pessoais[80], onde é introduzido o direito ao esquecimento.

Como vimos anteriormente a 24 de Outubro de 1995 entrou em vigor a Directiva 95/46/CE do Parlamento Europeu e do Conselho, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. No entanto, dela não constava o Direito ao Esquecimento que apenas surge pela primeira vez no processo de reforma da Directiva 95/46/CE, em 2012, na Comunicação da Comissão Europeia ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões: "Uma abordagem global da

[78] Vide CANAES, Carlos "Direito ao esquecimento em processo penal" disponivel em http://www.carloscanaes.pt/2014/07/24/direito-ao-esquecimento-em-processo-penal/acedido pela ultima vez a 13 de Julho de 2018.

[79] Vide Comunicado de Viviane Reding -The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age disponível em http://europa.eu/rapid/press-release_SPEECH-12-26_en.htm

[80] Regulamento (UE) 2016/679 Do Parlamento Europeu E Do Conselho de 27 de Abril de 2016 relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Protecção de Dados) disponível em: https://www.cncs.gov.pt/content/files/regulamento_ue_2016-679_-_protecao_de_dados.pdf

protecção de dados pessoais na União Europeia".[81] Sendo posteriormente apresentada uma proposta de Regulamento Geral sobre Protecção de Dados Pessoais [82]. Nesta comunicação a Comissão clarifica o Direito ao Esquecimento como "o direito de as pessoas impedirem a continuação do tratamento dos respectivos dados e de os mesmos serem apagados quando deixarem de ser necessários para fins legítimos. É o caso, por exemplo, do tratamento baseado o consentimento da pessoa, se essa pessoa retirar o consentimento ou quando o período de armazenamento tiver acabado"[83].

Vários foram os argumentos contra a proposta do regulamento mas sobretudo os argumentos relativos à liberdade de acesso à Internet e à falta de clareza sobre a forma como o direito ao esquecimento poderia ser.[84]

No RGPD encontramos tipificado o Direito ao Esquecimento no artigo 17º, na sua epígrafe: "Direito a ser esquecido e ao apagamento":

> *"1. O titular dos dados tem o direito de obter do responsável pelo tratamento o apagamento de dados pessoais que lhe digam respeito e a cessação da comunicação ulterior desses dados, especialmente em relação a dados pessoais que tenham sido disponibilizados pelo titular dos dados quando ainda era uma criança, sempre que se aplique um dos motivos seguintes:*
> *(a) Os dados deixaram de ser necessários em relação à finalidade que motivou a sua recolha ou tratamento;*
> *(b) O titular dos dados retira o consentimento sobre o qual é baseado o tratamento nos termos do artigo 6.o, n.o 1, alínea a), ou se o período de conservação consentido tiver terminado e não existir outro fundamento jurídico para o tratamento dos dados;*
> *(c) O titular dos dados opõe-se ao tratamento de dados pessoais nos termos do artigo 19.o;*
> *(d) O tratamento dos dados não respeita o presente regulamento por outros motivos."*[85]

O número 2 do mesmo artigo visa os motores de busca, sendo que no caso de este ter de apagar determinadas ligações deverá tomar medidas razoáveis para informar os

[81] Vide in Comunicado da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões: Protecção da privacidade num mundo interligado. Um quadro europeu de protecção de dados para o século XXI, COM (2012) 9 final, Bruxelas 25.1.2012

[82] Vide in "Proposta de regulamento do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados".

[83] Vide, Comunicação da Comissão ao Parlamento (…) op.cit. pag 8

[84] Vide Ghezzi , Alessia , Ângela Guimarães Pereira and Lucia Vesnić-Alujević The Ethics of Memory in a Digital Age - European Commisson, Joint Research Centre 2014

[85] Vide in Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)

responsáveis pelo tratamento dos dados que o titular dos dados lhes solícitou o apagamento das ligações.

### 4.4.6 Obrigação de notificação da rectificação ou apagamento dos dados pessoais ou limitação do tratamento

Este direito do titular encontra-se escrito na forma de obrigação para o responsável. No entanto, acreditamos que a epígrafe do artigo poderia também ser o "Direito do Titular dos dados em ser notificado da rectificação ou apagamento dos dados pessoais ou limitação do tratamento".

Segundo este artigo, o responsável pelo tratamento dos dados terá de comunicar ao titular dos dados caso tenha havido rectificação ou apagamento dos seus dados pessoais ou caso tenha existido uma limitação do tratamento desde que em conformidade com os artigo 16.º, o artigo 17.º, n.º 1, e o artigo 18º do regulamento. Esta notificação pode deixar de ser feita apenas se a comunicação se revelar impossível ou implicar um esforço desproporcionado. O responsável pelo tratamento terá ainda de fornecer ao titular informação sobre os destinatários se assim for solicitado pelo titular dos dados.[86]

### 4.4.7 Direito à portabilidade

O direito à portabilidade dos dados é um novo direito que surge com o regulamento geral de protecção de dados. Este direito, ainda que apenas efectivado com o RGPD, já havia sido mencionado na Resolução do Parlamento Europeu de 2011[87].

Este direito tem como objectivo possibilitar ao titular dos dados a transferência dos seus dados de forma fácil e célere de um prestador de serviços para outro. O que acontece aqui é que é facilitado ao titular dos dados a transmissão dos seus dados pessoais. O responsável pelo tratamento dos dados a quem foi pedida a portabilidade ficará obrigado a disponibilizar os dados a outro responsável, através de um formato que possa ser facilmente transferido para o novo prestador.

[86] Regulamento Geral de Protecção (…)op.cit.Art.19º.

[87] Resolução do Parlamento Europeu, de 6 de Julho de 2011, sobre uma abordagem global da protecção de dados pessoais na União Europeia disponível em: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2011-0323+0+DOC+XML+V0//PT acedido pela última vez a 28 de Julho de 2018.

O Direito de Portabilidade de Dados está contemplado no artigo 20º, nº 1, alíneas a) e b) do Regulamento Geral da Protecção de Dados, estatuindo que:

> *"1. O titular dos dados tem o direito de receber os dados pessoais que lhe digam respeito e que tenha fornecido a um responsável pelo tratamento, num formato estruturado, de uso corrente e de leitura automática, e o direito de transmitir esses dados a outro responsável pelo tratamento sem que o responsável a quem os dados pessoais foram fornecidos o possa impedir, se:*
>
> *a)O tratamento se basear no consentimento dado nos termos do artigo 6.o, n.o 1, alínea a), ou do artigo 9.o, n.o 2, alínea a), ou num contrato referido no artigo 6.o, n.o 1, alínea b); e*
>
> *b)O tratamento for realizado por meios automatizados.*
>
> *2. Ao exercer o seu direito de portabilidade dos dados nos termos do n.o 1, o titular dos dados tem o direito a que os dados pessoais sejam transmitidos diretamente entre os responsáveis pelo tratamento, sempre que tal seja tecnicamente possível.*
>
> *3. O exercício do direito a que se refere o n.o 1 do presente artigo aplica-se sem prejuízo do artigo 17.o. Esse direito não se aplica ao tratamento necessário para o exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento.*
>
> *4. O direito a que se refere o n.o 1 não prejudica os direitos e as liberdades de terceiros."*[88]

### 4.4.8 Direito à oposição

O direito à oposição é o direito que possibilita ao titular dos dados o direito de se opor a qualquer momento ao tratamento dos seus dados.

Embora o direito à oposição não seja um direito novo, o RGPD introduziu-nos algumas novidades no que concerne ao tratamento automatizado de dados sendo que no artigo 21º pode ler-se que "o titular dos dados tem o direito de se opor a qualquer momento(…) ao tratamento de dados pessoais que lhe digam respeito (..) incluindo a definição de perfis com base nessas disposições. O responsável pelo tratamento cessa o tratamento de dados pessoais, a não ser que apresente razões imperiosas e legítimas para esse tratamento que prevaleçam sobre os interesses, direitos e liberdades do titular de dados, ou para efeitos de declaração, exercício ou defesa de um direito num processo judicial" [89]

[88] Regulamento Geral de Protecção (…) op.cit. op.cit.Art.20º.

[89] Regulamento Geral de Protecção (…)op.cit.número 1 Art.21

O titular pode ainda exercer o seu direito à oposição quando o tratamento dos seus dados pessoais tenha o fim de comercialização directa tal como podemos ler no número 1 do artigo 21º do RGPD: "*quando os dados forem tratados para efeitos de comercialização directa, o titular dos dados tem o direito de se opor a qualquer momento ao tratamento dos dados pessoais que lhe digam respeito para os efeitos da referida comercialização, o que abrange a definição de perfis na medida em que esteja relacionada com a comercialização directa*"[90] sendo que se tal oposição se der, os dados pessoais deixam de poder ser tratados para essa finalidade. O titular pode ainda opor-se ao tratamento dos deus dados nos casos de investigação cientifica ou histórica ou para fins estatísticos. Este direito à oposição só não poderá ser exercido se o tratamento for necessário para a prossecução de atribuições de interesse público.

# 5 Obrigação dos intervenientes: RGPD vs Actores na *Cloud*

## 5.1 Responsável pelo Tratamento dos Dados (*controller*)

Falamos de Responsável pelo tratamento dos dados quando nos referimos à entidade que determina as finalidades e os meios do tratamento dos dados. Segundo o RGPD, o Responsável pelo tratamento poderá ser uma pessoa singular ou colectiva, autoridade pública, agência ou outro organismo que, "individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais"[91]
No caso das finalidades e os meios de tratamento serem definidos pelo direito da UE ou de um Estado-Membro "o responsável pelo tratamento ou os critérios específicos aplicáveis à sua nomeação podem ser previstos pelo direito da União ou de um Estado Membro".[92]
O Responsável pelo tratamento, individualmente ou em conjunto, deve celebrar um acordo que defina as responsabilidades pelo cumprimento das regras impostas pelo RGPD. Os principais aspectos desse acordo devem ser comunicados aos titulares dos dados, segundo o Direito à Informação que vimos anteriormente.

## 5.2 Subcontratante (*processor*)

[90] idem
[91] Regulamento Geral de Protecção (…)op.cit.Art 4º.
[92] Regulamento Geral de Protecção (…)op.cit.Art.4º.

Segundo o RGPD a figura do subcontratante trata de uma pessoa singular ou colectiva, a autoridade pública, agência ou outro organismo que proceda ao tratamento dos dados pessoais por conta de um responsável pelo tratamento, ou seja, o subcontratante só efectua o tratamento de dados pessoais em nome do responsável pelo tratamento. Por norma o subcontratante é externo à empresa. No entanto, no caso de grupos de empresas, uma empresa pode actuar como subcontratante para outra empresa do seu grupo.[93]

Os deveres do subcontratante perante o responsável pelo tratamento devem ser especificados num contrato ou noutro acto jurídico. Por exemplo, o contrato deve indicar o que acontece aos dados pessoais uma vez que este termine.

No que concerne a uma subcontratação por parte do subcontratante, este só o poderá fazer com uma autorização prévia do responsável pelo tratamento dos dados.

Definir a figura do subcontratante é particularmente importante no contexto da *cloud*. Iremos ver mais à frente como definir o papel do CSP, podendo este revestir a forma de responsável pelo tratamento dos dados ou subcontratante.

## 5.3 Terceiro

Segundo o regulamento geral de protecção de dados, o "Terceiro" é "a pessoa singular ou colectiva, a autoridade pública, o serviço ou organismo que não seja o titular dos dados, o responsável pelo tratamento, o subcontratante e as pessoas que, sob a autoridade directa do responsável pelo tratamento ou do subcontratante, estão autorizadas a tratar os dados pessoais".[94]

## 5.4 *Cloud Service Provider*: *Controller* ou *Processor*?

Em termos gerais *Cloud Service Provider* (CSP) será uma entidade que torna acessíveis os serviços *cloud*. Tal como existem fornecedores de água e luz, aqui o CSP funciona também ele como um fornecedor de serviços.

Ainda que ao serem colocados os dados na *cloud*, haja a percepção de tornar os dados públicos ou que exista uma perda de controlo sobre esses dados, os dados

[93] Regulamento Geral de Protecção (…) op.cit..Art.4º.

[94] Regulamento Geral De Protecção (…), art 4º.

pessoais continuam a estar protegidos. Tal como vimos anteriormente na definição do artigo 4º do RGPD, um dado pessoal é qualquer dado que torne uma pessoa identificável e assim sendo, ainda que na *cloud*, esse dado continua a estar sob a alçada e protecção do Regulamento bem como de outros instrumentos de protecção de dados.

Aqui o problema jaz não na definição de CSP mas sim no seu papel, existe uma dificuldade em perceber se o CSP é um Responsável pelo tratamento dos dados ou um subcontratante. A resposta a esta questão será: depende de cada situação em concreto, ou seja, o CSP actuará como subcontratante quando seja contratado por um responsável pelo tratamento e não trate os dados para seu próprio benefício, este será o caso mais recorrente. No entanto quando o CSP trata a informação para seu beneficio directo, então tal transformá-lo-á em responsável pelo tratamento. [95]

Alguns CSP definem o seu papel na política de privacidade, a Apple por exemplo assume na sua política o papel de responsável pelo tratamento, dizendo que "*Todas as informações que fornecemos podem ser transferidas ou acedidas por entidades em todo o mundo, conforme descrito nesta Política de Privacidade. As informações pessoais, relacionadas a serviços Apple, sobre indivíduos que residem em um Estado Membro do Espaço Económico Europeu (EEE) e na Suíça são controladas pela Apple Distribution International na Irlanda, e processadas em seu nome pela Apple Inc.*"[96]

Não obstante o que foi supramencionado, a opinião aqui é a de que o CSP, ainda que maioritariamente possa assumir o papel de subcontratante, será quase sempre também responsável pelo tratamento de alguns dados pessoais, na medida em que em geral qualquer CSP requer um login. Sendo esses dados considerados dados pessoais.

### 5.4.1 *Cloud Service Provider* como *Processor*

A Directiva 95/46/CE impunha várias obrigações apenas aos responsáveis pelo tratamento. Assim, no caso de o CSP actuar como um subcontratante através de um contrato com o responsável pelo tratamento, este era considerado responsável apenas pelo incumprimento do contrato. Ao contrário da Directiva, o RGPD é bastante claro

[95] Comissão Europeia "What is a data controller or a data processor?" disponível em https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_en, acedido pela ultima vez a 115 de Julho de 2018

[96] Politica de privacidade da Apple Inc, disponível em https://www.apple.com/legal/privacy/br/ acedido pela ultima vez a 11 de agosto de 2018

quanto às responsabilidades acrescidas do subcontratante, na medida em que refere no artigo 5º nº2: "O responsável pelo tratamento é responsável pelo cumprimento do disposto no n.º 1 e tem de poder comprová-lo ( «responsabilidade»)"[97].

> *"Para assegurar o cumprimento do presente regulamento no que se refere ao tratamento a efectuar pelo subcontratante por conta do responsável pelo tratamento, este, quando confiar actividades de tratamento a um subcontratante, deverá recorrer exclusivamente a subcontratantes que ofereçam garantias suficientes, especialmente em termos de conhecimentos especializados, fiabilidade e recursos, quanto à execução de medidas técnicas e organizativas que cumpram os requisitos do presente regulamento, nomeadamente no que se refere à segurança do tratamento. O facto de o subcontratante cumprir um código de conduta aprovado ou um procedimento de certificação aprovado poderá ser utilizado como elemento para demonstrar o cumprimento das obrigações do responsável pelo tratamento. A realização de operações de tratamento de dados em subcontratação deverá ser regulada por um contrato ou por outro ato normativo ao abrigo do direito da União ou dos Estados Membros, que vincule o subcontratante ao responsável pelo tratamento e em que seja estabelecido o objecto e a duração do contrato, a natureza e as finalidades do tratamento, o tipo de dados pessoais e as categorias dos titulares dos dados, tendo em conta as tarefas e responsabilidades específicas do subcontratante no contexto do tratamento a realizar e o risco em relação aos direitos e liberdades do titular dos dados. O responsável pelo tratamento e o subcontratante poderão optar por utilizar um contrato individual ou cláusulas contratuais-tipo que são adoptadas quer directamente pela Comissão quer por uma autoridade de controlo em conformidade com o procedimento de controlo da coerência e adoptadas posteriormente pela Comissão. Após concluído o tratamento por conta do responsável pelo tratamento, o subcontratante deverá, consoante a escolha do primeiro, devolver ou apagar os dados pessoais, a menos que seja exigida a conservação dos dados pessoais ao* abrigo do direito da União ou do Estado-Membro a que o subcontratante está sujeito."[98]

Como acima mencionado o RGPD trouxe bem mais responsabilidades para os subcontratantes que a Directiva, aplica-se agora também e directamente a eles a responsabilidade. Desta forma, a título de exemplo, os subcontratantes bem como os responsáveis pelo tratamento, devem manter registos escritos sobre todas as categorias de tratamento de dados pessoais e actividades realizadas em nome de um responsável pelo tratamento. Cabe tanto ao "responsável pelo tratamento e, sendo caso disso, ao subcontratante, ao representante do responsável pelo tratamento ou do subcontratante, disponibilizar, a pedido, o registo à autoridade de controlo."[99]

[97] Regulamento Geral de Protecção(…) art 5º nº2

[98] Regulamento Geral de Protecção(…) Art. Considerando 81

[99] Regulamento Geral de Protecção(…) op.cit. Art. 30 nº2 e nº 4.

No que concerne à cooperação entre estas entidades, estabelece o artigo 31º que "O responsável pelo tratamento e o subcontratante e, sendo caso disso, os seus representantes cooperam com a autoridade de controlo, a pedido desta, na prossecução das suas atribuições." [100]O GDPR contempla ainda a possibilidade de o subcontratante contratar outro subcontratante, diz-nos o número 2 do artigo 28º que o "subcontratante não contrata outro subcontratante sem que o responsável pelo tratamento tenha dado, previamente e por escrito, autorização específica ou geral. Em caso de autorização geral por escrito, o subcontratante informa o responsável pelo tratamento de quaisquer alterações pretendidas quanto ao aumento do número ou à substituição de outros subcontratantes, dando assim ao responsável pelo tratamento a oportunidade de se opor a tais alterações."[101]

Neste caso específico em que um subcontratante contrata outro subcontratante, o regulamente obrigada a que haja uma regulamentação por meio de um "contrato ou outro ato normativo ao abrigo do direito da União ou dos Estados-Membros, que vincule o subcontratante ao responsável pelo tratamento, estabeleça o objecto e a duração do tratamento, a natureza e finalidade do tratamento, o tipo de dados pessoais e as categorias dos titulares dos dados, e as obrigações e direitos do responsável pelo tratamento."[102] Nesse contrato deverão estar estabelecidos vários pontos sendo que o subcontratante:

> *" a) Trata os dados pessoais apenas mediante instruções documentadas do responsável pelo tratamento, incluindo no que respeita às transferências de dados para países terceiros ou organizações internacionais, a menos que seja obrigado a fazê-lo pelo direito da União ou do Estado-Membro a que está sujeito, informando nesse caso o responsável pelo tratamento desse requisito jurídico antes do tratamento, salvo se a lei proibir tal informação por motivos importantes de interesse público;*
>
> *b) Assegura que as pessoas autorizadas a tratar os dados pessoais assumiram um compromisso de confidencialidade ou estão sujeitas a adequadas obrigações legais de confidencialidade;*
>
> *c) Adopta todas as medidas exigidas nos termos do artigo 32.o;*
>
> *d) Respeita as condições a que se referem os n.os 2 e 4 para contratar outro subcontratante;*
>
> *e) Toma em conta a natureza do tratamento, e na medida do possível, presta assistência ao responsável pelo tratamento através de medidas técnicas e organizativas adequadas, para permitir que este cumpra a sua obrigação de dar resposta aos pedidos dos titulares dos dados tendo em vista o exercício dos seus direitos previstos no capítulo III;*
>
> *f) Presta assistência ao responsável pelo tratamento no sentido de assegurar o cumprimento das obrigações previstas nos artigos 32.o a 36.o,*

[100] Regulamento Geral de Protecção(…)op.cit. Art 31º.
[101] Regulamento Geral de Protecção(…)op.cit. Art 28 nº2
[102]Regulamento Geral de Protecção(…)op.cit. Art 28

*tendo em conta a natureza do tratamento e a informação ao dispor do subcontratante;*

*g) Consoante a escolha do responsável pelo tratamento, apaga ou devolve-lhe todos os dados pessoais depois de concluída a prestação de serviços relacionados com o tratamento, apagando as cópias existentes, a menos que a conservação dos dados seja exigida ao abrigo do direito da União ou dos Estados-Membros; e*

*h) Disponibiliza ao responsável pelo tratamento todas as informações necessárias para demonstrar o cumprimento das obrigações previstas no presente artigo e facilita e contribui para as auditorias, inclusive as inspecções, conduzidas pelo responsável pelo tratamento ou por outro auditor por este mandatado."*[103]

No número 4º deste mesmo artigo lê-se a sumula das responsabilidades no que diz respeito a um subcontratante contratar um segundo subcontratante, dizendo-nos que:

*" Se o subcontratante contratar outro subcontratante para a realização de operações específicas de tratamento de dados por conta do responsável pelo tratamento, são impostas a esse outro subcontratante, por contrato ou outro ato normativo ao abrigo do direito da União ou dos Estados-Membros, as mesmas obrigações em matéria de protecção de dados que as estabelecidas no contrato ou outro ato normativo entre o responsável pelo tratamento e o subcontratante, referidas no n.o 3, em particular a obrigação de apresentar garantias suficientes de execução de medidas técnicas e organizativas adequadas de uma forma que o tratamento seja conforme com os requisitos do presente regulamento. Se esse outro subcontratante não cumprir as suas obrigações em matéria de protecção de dados, o subcontratante inicial continua a ser plenamente responsável, perante o responsável pelo tratamento, pelo cumprimento das obrigações desse outro subcontratante."*[104]

[103] Regulamento Geral de Protecção (…) op.cit. número 2 Art 28
[104] Regulamento Geral de Protecção (…)op.cit. número 4 Art 28

# 6. *Data Security – Impact Assessments* e *Data Breach Notifications*

O RGPD trouxe claras e significativas mudanças no que concerne à segurança dos dados. Exige por exemplo que os responsáveis pelo tratamento apliquem medidas adequadas para assegurar e comprovar a conformidade com o RGPD.[105]

Ainda que os memorandos iniciais não tenham carácter vinculativo, é possível ler-se no memorando 83 que:

> "O responsável pelo tratamento deverá informar, sem demora injustificada, o titular dos dados da violação de dados pessoais quando for provável que desta resulte um elevado risco para os direitos e liberdades da pessoa singular, a fim de lhe permitir tomar as precauções necessárias. A comunicação deverá descrever a natureza da violação de dados pessoais e dirigir recomendações à pessoa singular em causa para atenuar potenciais efeitos adversos. Essa comunicação aos titulares dos dados deverá ser efectuada logo que seja razoavelmente possível, em estreita cooperação com a autoridade de controlo e em cumprimento das orientações fornecidas por esta ou por outras autoridades competentes, como as autoridades de polícia. Por exemplo, a necessidade de atenuar um risco imediato de prejuízo exigirá uma pronta comunicação aos titulares dos dados, mas a necessidade de aplicar medidas adequadas contra violações de dados pessoais recorrentes ou similares poderá justificar um período mais alargado para a comunicação."[106]

Isto leva à obrigação de conduzir o processo de Avaliações de Impacto (*Impact assessment*) e a uma obrigação de notificar caso exista uma violação de dados *(Data Breach*).

O artigo 32º do RGPD avança com medidas técnicas e organizativas adequadas para prover um nível de segurança que se adeqúe ao risco, sendo estas medidas[107]:

-A pseudoanonimização e a cifragem dos dados pessoais;

-A capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento;

-A capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico e;

[105] Regulamento Geral de Protecção (…) op.cit..numero 1 Art.24.
[106] Regulamento geral de Protecção (…) op.cit.considerando 83
[107] Regulamento Geral de Protecção (…) op.cit. Art 32º

-Um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento.

## 6.1 Violação de dados pessoais (Data breach)

O artigo 33º do Regulamento Geral de Protecção de Dados obrigada o responsável pelo tratamento dos dados a notificar a autoridade de controlo de qualquer violação de dados pessoais, sempre que possível, até no máximo 72 horas de ter tomado conhecimento de tal violação. Essa notificação não terá lugar apenas se a violação não resultar num risco para os direitos e liberdades dos titulares dos dados. O responsável do tratamento é ainda obrigado a fazer acompanhar a notificação dos motivos de atraso caso não faça essa notificação no período de 72 horas. A notificação deve descrever a natureza da violação dos dados pessoais, bem como comunicar o nome e os contactos do encarregado da protecção de dados, para além disso deve descrever as consequências prováveis da violação de dados pessoais e as medidas adoptadas ou propostas pelo responsável pelo tratamento para reparar a violação de dados pessoais. No entanto, as obrigações de notificação de "data breach" não são apenas para o responsável pelo tratamento de dados, também o subcontratante tem, segundo o número 2 do mesmo artigo, a obrigatoriedade de notificar o responsável pelo tratamento de dados após ter conhecimento de uma violação de dados pessoais.[108]

A comunicação ao titular dos dados de uma violação de dados pessoais, está contemplada no artigo 34º e apenas é obrigatória se for susceptível de "implicar um elevado risco para os direitos e liberdades das pessoas singulares "[109].

Esta obrigação não deve ser exigida se forem satisfeitas as seguintes condições:

" a) O responsável pelo tratamento tiver aplicado medidas de protecção adequadas, tanto técnicas como organizativas, e essas medidas tiverem sido aplicadas aos dados pessoais afectados pela violação de dados pessoais, especialmente medidas que tornem os dados pessoais incompreensíveis para qualquer pessoa não autorizada a aceder a esses dados, tais como a cifragem;

b) O responsável pelo tratamento tiver tomado medidas subsequentes que assegurem que o elevado risco para os direitos e liberdades dos titulares dos dados a que se refere o n.º 1 já não é susceptível de se concretizar; ou

[108] Regulamento Geral de Proeccção(…) op.cit. art.33.
[109] Regulamento Geral de Proeccção(…)op.cit. art.34.

c) Implicar um esforço desproporcionado. Nesse caso, é feita uma comunicação pública ou tomada uma medida semelhante através da qual os titulares dos dados são informados de forma igualmente eficaz." [110]

Estas obrigações devem ser descritas em acordo no contrato entre o responsável pelo tratamento dos dados e o titular dos dados.

## 6.2 Avaliação de Impacto (*Impact assessment*)

O RGPD introduz-nos no seu artigo 35º uma nova obrigação para o responsável pelo tratamento. O responsável, "quando um certo tipo de tratamento, em particular que utilize novas tecnologias e tendo em conta a sua natureza, âmbito e contexto e finalidade, for susceptível de implicar um elevado risco para os direitos e liberdades das pessoas singulares" deverá, antes de iniciar o tratamento dos dados, fazer uma avaliação do impacto das operações sobre os dados pessoais.[111]

A avaliação de impacto é obrigatória em caso de:

1) Avaliação sistemática de aspectos pessoais de titulares de dados, com base em tratamento automatizado, incluindo a definição de perfis. Sendo que com base nessa avaliação serão adoptadas decisões que produzem efeitos jurídicos para o titular;
2) Operações de tratamento em grande escala de categorias especiais de dados ou de dados pessoais relacionados com condenações penais e infracções;
3)Controlo sistemático de zonas acessíveis ao público em grande escala.[112]

A avaliação de impacto deverá incluir:

"1) Uma descrição sistemática das operações de tratamento previstas e a finalidade do tratamento, inclusive, se for caso disso, os interesses legítimos do responsável pelo tratamento;

2) Uma avaliação da necessidade e proporcionalidade das operações de tratamento em relação aos objectivos;

3)Uma avaliação dos riscos para os direitos e liberdades dos titulares dos direitos;

4)As medidas previstas para fazer face aos riscos, incluindo as garantias, medidas de segurança e procedimentos destinados a assegurar a protecção dos dados pessoais e demonstrar a conformidade com o presente regulamento, tendo em

[110] Regulamento Geral de Protecção (…)op.cit.Art. 33.
[111] Regulamento Geral de Protecção (…) op.cit.Art. 35.
[112] Regulamento Geral de Protecção (…) op.cit.Art. 35.

conta os direitos e os legítimos interesses dos titulares dos dados e de outras pessoas em causa."[113]

Depois de realizada a avaliação de impacto, o responsável pelo tratamento, se necessário, poderá fazer um controlo de forma a saber se o tratamento está a ser feito em conformidade com a avaliação de impacto .

# 7. Transferências para países terceiros

## 7.1 Perspectiva Global

Devido à nova era global, a recolha e partilha de dados pessoais atingiram um aumento quase exponencial. Como vimos anteriormente, as novas tecnologias propiciaram aos entes públicos e privados uma cada vez maior utilização de dados pessoais, sendo que o ónus não recai apenas nestes entes, mas também nos titulares dos dados que, de forma geral, em muito devido às redes sociais, divulgam os seus dados numa escala nunca antes vista. Toda esta evolução propiciou um enorme aumento na circulação de dados pessoais tanto dentro da União Europeia como para países terceiros. É assim vital que se consiga proceder a uma protecção desses dados.[114]Segundo o artigo 44º, que estabelece o princípio geral das transferências, as transferências de dados que sejam alvo de tratamento depois de transferidas para um país terceiro ou organização internacional, apenas se dão se respeitadas pelo responsável do tratamento de dados e subcontratantes das condições estabelecidas no RGPD.[115]

Quando as transferências se dão no seio da União Europeia, o nível de protecção dado por este regulamento, será garantido. A preocupação acresce quando se trata da protecção de dados transferidos para um país terceiro ou organizações internacionais. O que o regulamento enfatiza, e pode ser lido no memorando 101 é que as "transferências para países terceiros e organizações internacionais só podem ser efectuadas no pleno respeito pelo presente regulamento. Só poderão ser realizadas transferências se observadas as demais disposições do presente regulamento relativas a transferências de dados pessoais para países terceiros e organizações

[113] Regulamento Geral de Protecção(…) Art.35.
[114] Regulamento Geral de Portecção (…) Considerando 6
[115] Regulamento Geral de Portecção (…) Art 44º.

internacionais forem cumpridas pelo responsável pelo tratamento ou subcontratante."[116]

Aqui, a entidade que pode tomar a decisão de se um país terceiro ou organização internacional oferece ou não um nível de adequação à protecção de dados é a Comissão. Desta forma, existe uma segurança e uma uniformização jurídica na UE quanto a certo país terceiro ou organização internacional nos casos em que a Comissão considere que existe esse nível de adequação. No caso da decisão favorável da Comissão, podem então ser realizadas transferências de dados pessoais sem que haja necessidade de qualquer outra autorização.[117]

O nível de adequação segundo o memorando 104 assenta em vários factores, podendo ler-se:

> *"Em conformidade com os valores fundamentais em que a União assenta, particularmente a defesa dos direitos humanos, a Comissão deverá, na sua avaliação do país terceiro ou de um território ou sector específico de um país terceiro, ter em consideração em que medida esse país respeita o primado do Estado de direito, o acesso à justiça e as regras e normas internacionais no domínio dos direitos humanos e a sua legislação geral e sectorial, nomeadamente a legislação relativa à segurança pública, à defesa e à segurança nacional, bem como a lei da ordem pública e a lei penal. A adopção de uma decisão de adequação relativamente a um território ou um sector específico num país terceiro deverá ter em conta critérios claros e objectivos, tais como as actividades de tratamento específicas e o âmbito das normas jurídicas aplicáveis, bem como a legislação em vigor no país terceiro. Este deverá dar garantias para assegurar um nível adequado de protecção essencialmente equivalente ao assegurado na União, nomeadamente quando os dados pessoais são tratados num ou mais sectores específicos. Em especial, o país terceiro deverá garantir o controlo efectivo e independente da protecção dos dados e estabelecer regras de cooperação com as autoridades de protecção de dados dos Estados-Membros, e ainda conferir aos titulares dos dados direitos efectivos e oponíveis e vias efectivas de recurso administrativo e judicial."*

Este memorando encontra-se legalmente justificado no artigo 45º.

Após avaliar a adequação do nível de protecção, a Comissão pode decidir, através de um ato de execução, que um país terceiro, um território ou um ou mais sectores específicos de um país terceiro, ou uma organização internacional, garante um nível de protecção adequado. Não tendo sido tomada qualquer decisão nesse sentido, os responsáveis pelo tratamento ou subcontratantes só podem transferir dados pessoais para um país terceiro ou uma organização internacional se tiverem apresentado

[116] Regulamento Geral de Protecção (…) Considerando 101.
[117] Regulamento Geral de Protecção (…) Considerando 103.

garantias adequadas, e na condição de os titulares dos dados gozarem de direitos oponíveis e de medidas jurídicas correctivas eficazes.[118]

A Comissão poderá em todo o caso revogar a decisão reconhecendo que o país terceiro ou organização internacional deixou de prover os níveis de adequação. Deixará desta forma, de ser válida a transferência de dados pessoais para este país ou organização. No entanto, se os requisitos do regulamento no que concerne às transferências forem adequados, e apenas existam algumas derrogações para situações especificas, então poderá a Comissão juntamente com o país terceiro realizar consultas com o objectivo de fazer algumas correcções.[119]

Na falta de uma decisão sobre o nível de protecção adequado, o responsável pelo tratamento ou o subcontratante deverá adoptar as medidas necessárias para colmatar a insuficiência da protecção de dados no país terceiro, dando para tal garantias adequadas ao titular dos dados. Tais garantias adequadas podem consistir no recurso a regras vinculativas aplicáveis às empresas, cláusulas-tipo de protecção de dados adoptadas pela Comissão, cláusulas-tipo de protecção de dados adoptadas por uma autoridade de controlo, ou cláusulas contratuais autorizadas por esta autoridade. Essas medidas deverão assegurar o cumprimento dos requisitos relativos à protecção de dados e o respeito pelos direitos dos titulares dos dados adequados ao tratamento no território da União, incluindo a existência de direitos do titular de dados e de medidas jurídicas correctivas eficazes, nomeadamente o direito de recurso administrativo ou judicial e de exigir indemnização, quer no território da União quer num país terceiro. Deverão estar relacionadas, em especial, com o respeito pelos princípios gerais relativos ao tratamento de dados pessoais e pelos princípios de

[118]Podem ler-se no nº 2 do artigo as garantias adequadas.
"Sem requerer nenhuma autorização específica de uma autoridade de controlo, por meio de:
a)Um instrumento juridicamente vinculativo e com força executiva entre autoridades ou organismos públicos;
b)Regras vinculativas aplicáveis às empresas em conformidade com o artigo 47.o;
c)Cláusulas-tipo de protecção de dados adoptadas pela Comissão pelo procedimento de exame referido no artigo 93.o, n.o 2;
d)Cláusulas-tipo de protecção de dados adoptadas por uma autoridade de controlo e aprovadas pela Comissão pelo procedimento de exame referido no artigo 93.o, n.o 2;
e)Um código de conduta, aprovado nos termos do artigo 40.o, acompanhado de compromissos vinculativos e com força executiva assumidos pelos responsáveis pelo tratamento ou pelos subcontratantes no país terceiro no sentido de aplicarem as garantias adequadas, nomeadamente no que respeita aos direitos dos titulares dos dados; ou
f)Um procedimento de certificação, aprovado nos termos do artigo 42.o, acompanhado de compromissos vinculativos e com força executiva assumidos pelos responsáveis pelo tratamento ou pelos subcontratantes no país terceiro no sentido de aplicarem as garantias adequadas, nomeadamente no que respeita aos direitos dos titulares dos dados.
a)Cláusulas contratuais entre os responsáveis pelo tratamento ou subcontratantes e os responsáveis pelo tratamento, subcontratantes ou destinatários dos dados pessoais no país terceiro ou organização internacional; ou
b)Disposições a inserir nos acordos administrativos entre as autoridades ou organismos públicos que contemplem os direitos efectivos e oponíveis dos titulares dos dados."
[119] Regulamento Geral de Protecção (…) op.cit. Considerando 107

protecção de dados desde a concepção e por defeito. Também podem ser efectuadas transferências por autoridades ou organismos públicos para autoridades ou organismos públicos em países terceiros ou para organizações internacionais que tenham deveres e funções correspondentes, nomeadamente com base em disposições a inserir no regime administrativo, como seja um memorando de entendimento, que prevejam a existência de direitos efectivos e oponíveis dos titulares dos dados. Deverá ser obtida a autorização da autoridade de controlo competente quando as garantias previstas em regimes administrativos não forem juridicamente vinculativas.[120]

As empresas ou os grupos de empresas envolvidas numa actividade económica conjunta deverão poder utilizar as regras vinculativas aplicáveis às empresas aprovadas para as suas transferências internacionais da União para entidades pertencentes ao mesmo grupo empresarial ou grupo de empresas envolvidas numa actividade económica conjunta, desde que essas regras incluam todos os princípios essenciais e direitos oponíveis que visem assegurar garantias adequadas às transferências ou categorias de transferências de dados pessoais. O artigo que regula em matéria de empresas é o artigo 47º.[121]

## 7.2 Derrogações

A previsão das derrogações à falta de decisão de adequação ou de garantias adequadas está descrita no artigo 49º no RGPD. Desta forma deverá prever-se o consentimento do titular para a transferência dos dados, segundo a alínea a) do artigo 49º " Se titular dos dados tiver explicitamente dado o seu consentimento à transferência prevista, após ter sido informado dos possíveis riscos de tais transferências para si próprio devido à falta de uma decisão de adequação e das garantias adequadas".[122]

Há que prever também as situações em que a transferência de dados seja necessária para a "celebração ou execução de um contrato, celebrado entre o titular dos dados e o responsável pelo tratamento"[123] ou um contrato "celebrado no interesse do titular dos

[120] Regulamento Geral de Protecção (…) op.cit. Considerando 108
[121] Regulamento Geral de Protecção (…) op.cit. . Art 47
[122] Regulamento Geral de Protecção (…) op.cit. .Art. 49º nº1 a).
[123] Regulamento Geral de Protecção (…) op.cit. Art. 41º nº1 b).

dados, entre o responsável pelo seu tratamento e outra pessoa singular ou colectiva"[124]

Uma outra derrogação acontece quando a "transferência for necessária por importantes razões de interesse público"[125], sendo esse interesse público reconhecido pelo direito da UE ou direito do Estado Membro a que esteja sujeito o responsável pelo tratamento.[126] É também permitido caso a transferência seja necessária à declaração, ao exercício ou à defesa de um direito num processo judicial[127] ou para que sejam protegidos os interesses vitais do titular dos dados "[128]-[129]

Uma outra derrogação presente no número 1 do artigo 49º do RGPD diz respeito a transferências que sejam realizadas a partir de um registo que pelo Direito da UE ou Direito interno de um Estado "se destine a informar o público e se encontre aberto à consulta do público em geral ou de qualquer pessoa que possa provar nela ter um interesse legítimo[130]. No entanto, esta permissão não diz respeito à totalidade dos dados nem a categorias completas de dados pessoais constantes do registo. Quando o registo for consultado com base em interesse legítimo, as transferências só poderão ser realizadas a pedido dessas mesmas pessoas ou se forem seus destinatários, tendo em conta os interesses e os direitos fundamentais do titular dos dados [131].

Por fim, quando não for aplicável nenhuma das derrogações acima mencionadas, as transferências que se qualifiquem como não sendo repetitivas e que apenas digam respeito a um número limitado de titulares de dados, podem ser admitidas "*para efeitos dos interesses legítimos do responsável pelo tratamento, desde que esses interesses não se sobreponham aos interesses, direitos e liberdades do titular dos dados. O responsável pelo tratamento deverá atender especialmente à natureza dos dados pessoais, à finalidade e à duração da operação ou operações de tratamento previstas, bem como à situação vigente no país de origem, no país terceiro e no país de destino final, e deverá apresentar as garantias adequadas para defender os direitos*

[124] Regulamento Geral de Protecção (…) op.cit. .Art. 49º nº1 c).
[125] Regulamento Geral de Protecção (…) op.cit. Art. 49º nº1 d).
[126] Regulamento Geral de Protecção (…) op.cit..Art. 49º nº4.
[127] Regulamento Geral de Protecção (…) op.cit..Art. 49º nº1 e).
[128] Regulamento Geral de Protecção (…) op.cit..Art. 49º nº1 f).
[129] "Também se aplica para proteger os interesses vitais de outras pessoas, se esse titular estiver física ou legalmente incapaz de dar o seu consentimento"
[130] Regulamento Geral de Protecção (…) op.cit. op.cit.Art. 49º nº1 g).
[131] Regulamento Geral de Protecção (…) op.cit. op.cit.número 2 Art 49.

*e liberdades fundamentais das pessoas singulares relativamente ao tratamento dos seus dados pessoais."*[132]

## 7.3. Transferências entre a UE e os EUA

### 7.3.1 Porto Seguro (*Safe Harbor*)

Em Julho de 2000 foi adoptada uma decisão, chamada de "Porto Seguro"[133] (Safe Habour Decision), cujo objectivo era conferir um nível de protecção adequado às transferências de dados pessoais da UE para as organizações estabelecidas nos EUA. Assim, segundo esta decisão foi permitido um fluxo de dados pessoais entre os Estados da UE e entidades dos EUA que estivessem certificadas pelo "porto seguro". Se não existisse essa certificação, a transferência não se poderia dar visto que não respeitaria as normas da UE no que concerne à adequação do nível de protecção de dados.

A decisão "Porto Seguro" viria no entanto, anos mais tarde a ser de invalidada pelo acórdão Sherms.

Maximillian Schrems pelo direito que lhe era reconhecido pelo "Porto Seguro", pediu ao *Facebook* uma cópia de todos os dados que a empresa tivesse sobre si. O *Facebook* disponibilizou-lhe a descrição detalhada de toda a sua actividade na rede social desde a sua adesão, onde eram disponibilizadas informações sobre os amigos, convites de eventos e respostas, endereços de *e-mails* de contactos dos seus amigos e todas as conversas de chat.[134]

Uma vez que é na Irlanda que está localizada a filial europeia do *Facebook*, Schrems decidiu denunciar a situação ao *Data Protection Commissioner* da Irlanda, alegando que o *Facebook* retia informação que os utilizadores tinham eliminado e que a National Security Agency tinha acesso aos dados pessoais dos utilizadores da UE que estavam no *Facebook*. No entanto, o *Comissioner* arquivou a queixa, argumentando que não

[132] Regulamento Geral de Protecção (…) op.cit. op.cit.Considerando 113 e art 49nº1

[133] Decisão 520/2000/CE

[134]TJUE, "O Tribunal de Justiça declara inválida a decisão da Comissão que constatou que os Estados Unidos asseguram um nível de proteção adequado dos dados pessoais transferidos Tribunal de Justiça da União Europeia. Comunicado De Imprensa n° 117/15" Luxemburgo, 6 de Outubro de 2015 disponível em https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117pt.pdf, acedido pela ultima vez a 09 de Agosto de 2018.

seria da sua competência e visto considerar que não existiam provas de que a NSA tivesse tido acesso aos dados pessoais de Schrems.[135]

Não contente com o arquivo do caso, Scherms interpôs recurso da decisão em causa para o Supremo Tribunal de Justiça da Irlanda.[136] Este declarou que os dados pessoais transferidos da UE para os EUA teriam finalidades de interesse público. No entanto, o tribunal admitiu que não existia um direito dos titulares dos dados a serem ouvidos, visto alguns procedimentos de intercepção de dados serem secretos, impedindo os cidadãos europeus de contestarem os "excessos consideráveis" em matéria de protecção de dados, cometidos pela Agência de Segurança Nacional ou outros órgãos públicos [137]. O tribunal considerou ainda que se deveria analisar o caso à luz do Direito Comunitário, nomeadamente arts. 7.º, 8.º e 47.º da Carta e dos arts. 25.º, n.º 6, e 28.º da Directiva[138]

O TJUE observou que a decisão de adequação da Comissão não era suficiente no que concerne à equivalência de adequação de protecção de dados entre os EUA e a UE. Acrescendo ainda o facto da decisão "Porto Seguro*"* contemplar utilização dos dados por razões de interesse público, abrindo assim uma brecha a uma ingerência nos direitos dos titulares dos dados, podendo assim, as autoridades dos EUA aceder a dados pessoais da UE sem estar em conformidade com a decisão do "Porto Seguro". Acresce ainda como dito acima que não existiam vias de os cidadãos poderem recorrer a autoridades de forma a garantir a protecção dos seus dados pessoais, ou seja, é infringido o direito fundamental a uma tutela jurisdicional. Por último, um outro grande problema surge pelos reduzidos poderes das autoridades nacionais para poderem apreciar o nível de protecção de dados efectuado pelos EUA no âmbito da decisão "Porto Seguro", quando na verdade as autoridades de controlo deveriam

[135] O Tribunal de Justiça declara inválida a decisão da Comissão(…) op.cit.

[136] Acórdão Do Tribunal De Justiça (Grande Secção) 6 de Outubro de 2015 " Reenvio prejudicial — Dados pessoais — Protecção das pessoas singulares no que diz respeito ao tratamento desses dados — Carta dos Direitos Fundamentais da União Europeia — Artigos 7.°, 8.° e 47.° — Diretiva 95/46/CE — Artigos 25.° e 28.° — Transferência de dados pessoais para países terceiros — Decisão 2000/520/CE — Transferência de dados pessoais para os Estados Unidos — Nível de protecção inadequado — Validade — Queixa de uma pessoa singular cujos dados foram transferidos da União Europeia para os Estados Unidos — Poderes das autoridades nacionais de controlo". Doravante mencionado como Acórdão Scherms.

[137] Acórdão Schrems §31 que afirma que : "segundo esse mesmo órgão jurisdicional, os cidadãos da União não dispõem de nenhum direito efectivo a ser ouvidos. A supervisão das acções dos serviços de informações é feita através de procedimentos secretos e não contraditórios. Após a transferência de dados pessoais para os Estados Unidos, a NSA e outros órgãos federais, como o Federal Bureau of Investigation (FBI), podem aceder a tais dados no âmbito da vigilância e das interceções indiscriminadas a que procedem em grande escala".

[138] Acórdão Schrems §34 .

analisar se as transferências realizadas ao abrigo do "Porto Seguro" obedeciam ou não às exigências da antiga Directiva[139].

Desta forma e pelas razões acimas expostas, o TJUE declarou a invalidade da Decisão "Porto Seguro" no Acórdão Schrems.

### 7.3.2 Escudo de Privacidade (*Privacy Shield*)

Após a declaração de invalidade da decisão "Porto Seguro", a UE e os EUA começaram a negociar um outro documento de forma a garantir os níveis de protecção adequada da transferência de dados da EU para os EUA. Este foi um problema sério para muitas empresas e também afectou os CSP.

Foi assim emitido um novo documento apelidado de "Escudo de Privacidade" devendo este reflectir os requisitos estabelecidos pelo TJUE na decisão do "caso Schrem". [140]

Esta *framework* tem por objectivo fornecer às empresas de ambos os lados do Atlântico um mecanismo que cumpra os requisitos de adequação de protecção de dados aquando da transferência de dados pessoais da União Europeia e da Suíça para os Estados Unidos. A 12 de Julho de 2016, a Comissão Europeia[141] considerou o

[139] O Tribunal de Justiça declara inválida a decisão da Comissão (…)

[140]Vide VOSS, W. Gregory "European Union Data Privacy Law Reform: General Data Protection Regulation, Privacy Shield, and the Right to Delisting" p.1

[141] Em Fevereiro de 2016 a Comissão emitiu uma press release, de onde fez constar as garantias dadas pelos EUA, sendo estas:" - strong obligations on companies and robust enforcement: the new arrangement will be transparent and contain effective supervision mechanisms to ensure that companies respect their obligations, including sanctions or exclusion if they do not comply. The new rules also include tightened conditions for onward transfers to other partners by the companies participating in the scheme.
- clear safeguards and transparency obligations on U.S. government access: for the first time, the U.S. government has given the EU written assurance from the Office of the Director of National Intelligence that any access of public authorities for national security purposes will be subject to clear limitations, safeguards and oversight mechanisms, preventing generalised access to personal data. U.S. Secretary of State John Kerry committed to establishing a redress possibility in the area of national intelligence for Europeans through an Ombudsperson mechanism within the Department of State, who will be independent from national security services. The Ombudsperson will follow-up complaints and enquiries by individuals and inform them whether the relevant laws have been complied with. These written commitments will be published in the U.S. federal register.
- Effective protection of EU citizens' rights with several redress possibilities: Complaints have to be resolved by companies within 45 days. A free of charge Alternative Dispute Resolution solution will be available. EU citizens can also go to their national Data Protection Authorities, who will work with the Federal Trade Commission to ensure that unresolved complaints by EU citizens are investigated and resolved. If a case is not resolved by any of the other means, as a last resort there will be an arbitration mechanism ensuring an enforceable remedy. Moreover, companies can commit to comply with advice from European DPAs. This is obligatory for companies handling human resource data.
- Annual joint review mechanism: the mechanism will monitor the functioning of the Privacy Shield, including the commitments and assurance as regards access to data for law enforcement and national

o *Privacy Shield* adequado para permitir transferências de dados ao abrigo da legislação da UE e em 12 de Janeiro de 2017, o governo suíço anunciou a aprovação da Swiss-U.S. Privacy Shield Framework como um mecanismo legal válido para cumprir os requisitos suíços de transferência dados pessoais da Suíça para os Estados Unidos.[142]

O *privacy shield* permite desta forma organizações com base nos EUA possam certificar-se na *framework* e fazer transferências de dados de acordo com os princípios de adequação da EU e da Suíça. [143]

Em Setembro de 2017 deu-se a primeira revisão anual do *Privacy shield*, com base nessa revisão a comissão publico a 18 de Outubro de 2017 um relatório designado de "Report From The Commission To The European Parliament And

The Councilon The First Annual Review Of The Functioning Of The Eu–U.S. Privacy Shield".[144]

Nesse relatório a Comissão conclui que os Estados Unidos continuam a garantir um nível adequado de protecção dos dados pessoais da UE para organizações nos Estados Unidos.

A Comissão considerou ainda que a aplicação do Privacy Shield pode ser melhorada fazendo desta forma algumas recomendações.

As primeiras três recomendações dizem respeito ao Departamento de Comercio dos EUA, DoC. Primeiramente a Comissão considerou que o facto de empresas que fazem o pedido para o certificado do *privacy shield,* e que não obstante ainda não terem essa certificação finalizada e certificada pela DoC, poderem fazer uso desta, dá incerteza de níveis de adequação para as entidades e empresas da EU que pretendem fazer transferências para os EUA. Desta forma a Comissão dá a recomendação de que as empresas não poderão assim fazer uso da certificação antes

---

security purposes. The European Commission and the U.S. Department of Commerce will conduct the review and associate national intelligence experts from the U.S. and European Data Protection Authorities. The Commission will draw on all other sources of information available, including transparency reports by companies on the extent of government access requests. The Commission will also hold an annual privacy summit with interested NGOs and stakeholders to discuss broader developments in the area of U.S. privacy law and their impact on Europeans. On the basis of the annual review, the Commission will issue a public report to the European Parliament and the Council." European Commission - Press release Restoring trust in transatlantic data flows through strong safeguards: European Commission presents EU-U.S. Privacy Shield, Brussels, 29 February 2016, disponivel em http://europa.eu/rapid/press-release_IP-16-433_en.htm , acedido pela última vez a 09 de Setembro de 2018.

[142] International Trade administration "Privacy Shield Program Overview" disponível em: https://www.privacyshield.gov/Program-Overview acedido pela ultima vez a 20 de Agosto de 2018.

[143] International Trade administration "Privacy Shield Program(…)op.cit.

[144] Comission, "Report From The Commission To The European Parliament And the Council on The First Annual Review Of The Functioning Of The Eu–U.S. Privacy Shield", Brusselas, 18 do 10 de 2017 , disponivel em https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/eu-us-privacy-shield_en#documents, acedido pela última vez a 23 de Outubro de 2018.

desta ser finalizada e revista pelo DoC. A segunda recomendação direcciona o DoC a conduzir revisões periódicas de forma a identificar entidades que tenham falsas certificações do privacy shield. Por último a Comissão recomenda ainda ao DoC fazer monotorização e vistorias a empresas com certificação, para fins de uma continua conformidade com o regulamento.[145]

São feitas depois recomendações para que seja criada um maior nível de consciencialização para a temática e cooperação entre as entidades. A Comissão compromete-se ainda a levar a cabo um estudo quando a decisões automatizadas tidas nas transferências feitas com base no *privacy shield.*

As últimas recomendações dizem respeito a leis internas dos EUA como a Foreign Intellifence Survaillance Act e a Presidencial Policy Directive terem em consideração e aumentarem o seu nível de protecção da privacidade. Pedindo ainda às autoridades competentes relatórios frequentes sobre quaisquer avanços que digam respeito e tenham relevância no quadro do *privacy shield*.[146]

[145] Comission, "Report From The Commission To The European Parliament And The Council on The First Annual Review Of The Functioning Of The Eu–U.S (...) pp 4-5.
[146] Comission, "Report From The Commission To The European Parliament And The Council on The First Annual Review Of The Functioning Of The Eu–U.S (...) pp 6-7.

# 8. Conclusão

Como vimos anteriormente a nova era digital levou a uma exponencial troca de dados e informação pessoal. Desde há muito que os Estados demonstraram preocupação em proteger a informação com um especial enfase na informação pessoal. A presente tese foca-se numa contextualização de toda a legislação entorno da protecção de dados pessoais na União Europeia. Ao mesmo tempo que a legislação começou a ser mais focada para a protecção da informação do individuo o fenómeno da cloud entrou nas nossas empresas, nas nossas casas e na vida de todos os cidadãos.

Para além desta problemática existe o risco de que sempre que a informação é transferida do espaço da União Europeia, o titular dos dados não consiga não possam exercer os seus direitos sobre a essa informação.

## Contributos:

Como contributo essencial, a presente dissertação foca-se no impacto do regulamento geral de protecção de dados na informação pessoal na cloud. Sendo que as responsabilidades dos *Cloud Service Providers* poderão variar consoante este seja visto como um subcontratante ou responsável pelo tratamento dos dados. Até então a Directiva que vigorava centrava-se apenas nas responsabilidades do Responsável pelo tratamento de dados, no entanto o novo regulamento veio trazer toda uma nova visão do ponto vista da responsabilidade sobre os subcontratantes.

Para além de uma análise detalhada da bibliografia bem como da regulamentação existente neste paradigma na presente tese é feito um contributo sobre do ponto de vista do papel dos *Could Service Providers*, que acreditamos que em muitas situações revistam tanto a forma de responsável pelo tratamento dos dados bem como de subcontratantes.

Foi ainda feita uma análise da jurisprudência existente no ramo da protecção de dados no escopo de traslações transatlânticas, constatando-se que aquando da antiga decisão do Porto Seguro as autoridades de controlo não eram capazes de fazer seguir quaisquer a reclamações ou investigações que não estivessem no seu âmbito

territorial. Analisando a nova Decisão do Escudo de protecção continuamos a acreditar que é essencial uma maior cooperação entre autoridades de controlo

## Desenvolvimentos Futuros:

No que concerne à transferência de dados para países terceiros de forma a assegurar uma maior protecção para o titular dos dados, a União Europeia bem como outras instituições continuam a trabalhar arduamente na promoção de uma cooperação mais próxima entre as autoridades de controlo de forma a conseguirem levar a cabo investigações no âmbito da protecção de dados com outras autoridades de controlo quando haja uma transferência. Assim continuam a ser feitos trabalhos na criação de regras no que diz respeito a facilitação na cooperação entre estas entidade.

## Biografia


- Amazon “o que é o cloud Computing”;

- AUSTRIA THE FEDERAL CONSTITUTIONAL LAW OF 1920 as amended in 1929 as to Law No. 153/2004, December 30, 2004;

- BUYYA, BRIBERG, GOSCINKI “*Cloud computing : principles and paradigms* , John Wiley & Sons, Inc 2011;

- COHEN FRED & Associates *A Short History of Cryptography*, p3 IBM, “what is Cloud Computing” ;

- COMITE DE MINISTROS*, Resolution (73) 22 On The Protection Of The Privacy Of Individuals Vis-A-Vis Electronic Data Banks In The Private Sector*;

- COMITE DE MINISTROS*, Resolution (74) 29 On The Protection Of The Privacy Of Individuals Vis-À-Vis Electronic Data Banksin The Public Sector;*

- COMISSÃO EUROPEIA “What is a data controller or a data processor?”;

- COMISSÃO EUROPEIA, Comunicado da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões: *Protecção da privacidade num mundo interligado. Um quadro europeu de protecção de dados para o século XXI, COM (2012) 9 final;*

- COMISSÃO EUROPEIA, Report From The Commission To The European Parliament And The Council on The First Annual Review Of The Functioning Of The Eu–U.S. Privacy Shield”, Brussels, 18 do 10 de 2017 .

- CONGRESO LOS DIPUTADOS Y DEL SENADO, CONSTITUICÍON ESPAÑOLA, Aprobada por Las Cortes en sesiones plenarias del Congreso los Diputados y del Senado celebradas el 31 de octubre de 1978, Ratificada por el pueblo español en referéndum de 6 de diciembre de 1978, Sancionada por S. M. el Rey ante Las Cortes el 27 de diciembre de 1978;

- CONSELHO DA EUROPA, Convenção para a Protecção das Pessoas Relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal, 1981;

- CANAES, Carlos *Direito ao esquecimento em processo penal*;

- CONSELHO DA EUROPA, Convenção Europeia dos Direitos Humanos, 1950;

- CONSELHO DA EUROPA, Protocolo Adicional À Convenção Para A Protecção Das Pessoas Relativamente Ao Tratamento Automatizado De Dados De Carácter Pessoal, Respeitante Às Autoridades De Controlo E Aos Fluxos Transfronteiriços De Dados, 1981;

- EUROPEAN COMISSION - Press release - Restoring trust in transatlantic data flows through strong safeguards: European Commission presents EU-U.S. Privacy Shield, Brussels, 2016;

- EUROPEAN COMMISSION, *European commission presents EU-U.S. Privacy Shield, Brussels, 29 February 2016*.

- FOOTE, Keith D. *A Brief History of Cloud Computing*;

- GHEZZI , ALESSIA , PEREIRA Ângela Guimarães and VESNIĆ-ALUJEVIĆ Lucia, *The Ethics of Memory in a Digital Age* - European Commisson, Joint Research Centre 2014;

- INTERNATIONAL TRADE ADMINISTRATION “Privacy Shield Program Overview”

- IPM SISTEMAS , *História da computação em nuvem: como surgiu a cloud computing?;*

- MELL Peter, GRANCE Timothy . The NIST Definition of Cloud Computing"p.7

- NAÇÕES UNIDAS *Declaração Universal dos Direitos do Homem*;

- ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÓNICO Directrizes da OCDE para a Protecção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais pp 5 e 6;

- PARLAMENTO EUROPEU E CONSELHO, Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados;

- PARLAMENTO EUROPEU E CONSELHO, *Proposta relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados;*

- PARLAMENTO EUROPEU, *Resolução do Parlamento Europeu, de 6 de Julho de 2011, sobre uma abordagem global da protecção de dados pessoais na União Europeia*;

- PARLAMENTO EUROPEU, Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados);

- REPÚBLICA PORTUGUESA, Constituição da RepublicaDecreto de aprovação da Constituição, Diário da República n.º 86/1976, Série I de 1976-04-10;

- SILVA Heraclides "A Protecção De Dados Pessoais Na Era Global: O Caso Schrems", Faculdade de Direito Universidade Nova de Lisboa 2017.

- TRIBUNAL DE JUSTIÇA (Grande Secção) , Acórdão de 6 de outubro de 2015 “ Reenvio prejudicial — Dados pessoais — Protecção das pessoas singulares no que diz respeito ao tratamento desses dados — Carta dos Direitos Fundamentais da União Europeia — Artigos 7.°, 8.° e 47.° — Diretiva 95/46/CE — Artigos 25.° e 28.° — Transferência de dados pessoais para países terceiros — Decisão 2000/520/CE — Transferência de dados pessoais para os Estados Unidos — Nível de protecção inadequado — Validade — Queixa de uma pessoa singular cujos dados foram transferidos da União Europeia para os Estados Unidos — Poderes das autoridades nacionais de controlo”;

- TJUE, “O Tribunal de Justiça declara inválida a decisão da Comissão que constatou que os Estados Unidos asseguram um nível de protecção adequado dos dados pessoais transferidos Tribunal de Justiça da União Europeia. Comunicado De Imprensa n° 117/15” Luxemburgo, 6 de Outubro de 2015 ;

- UNIÃO EUROPEIA Carta Dos Direitos Fundamentais 2012/C 326/02 ;

- VIVIANE REDING Comunicado -The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age ;

- VOSS, W. Gregory “European Union Data Privacy Law Reform: General Data Protection Regulation, Privacy Shield, and the Right to Delisting”.