Proteção de dados pessoais e RGPD

BE SAFE ON THE INTERNET

Co-funded by the Erasmus+ Programme of the European Union

Índice

Lista de abreviaturas

DPA: Autoridade de Proteção de Dados

DPO: Data Protection Officer

DSG: Lei de Proteção de Dados austríaca *Datenschutzgesetz*

DSVGO: *Datenschutz-Grundverordung* alemã

EEE: Espaço Económico Europeu

ePR: Regulamento *ePrivacy*

UE: União Europeia

RGPD: Regulamento Geral sobre a Proteção de Dados

Figuras

Tabelas

1. Introdução

Atualmente, o mundo depende cada vez mais de dados (pessoais ou não pessoais) em resultado do elevado valor acrescentado que estes podem acrescentar a diferentes agentes económicos. Na União Europeia (UE) exigem dois regulamentos referentes ao tratamento de dados pessoais: o Regulamento (UE) 2016/679 (Regulamento Geral sobre a Proteção de Dados) e o *ePrivacy* (ePR) que apresenta uma proposta para a Diretiva relativa à privacidade e às comunicações eletrónicas (Diretiva *ePrivacy* 2002/58/EC).

O Regulamento (UE) 2018/1807 tem como objetivo remover obstáculos referentes ao livre fluxo de dados não pessoais entre os estados-membros da UE e as Tecnologia de Informação na Europa. Juntamente com o Regulamento Geral sobre a Proteção de Dados (RGPD), o Regulamento (EU) 2018/1807 apresenta uma abordagem coerente e compreensiva sobre o livre fluxo de informação no território da UE. O objetivo do ePR passa por assegurar a confiança e a segurança no mercado digital único através da atualização do enquadramento legal da privacidade digital.

Os três regulamentos referidos anteriormente aplicam-se em todos os países europeus, apesar de existirem cláusulas que atribuem alguma liberdade legislativa a nível nacional.

No presente relatório é possível consultar informação relevante relacionada com a legislação que abrange o tratamento de dados pessoais e não pessoais. Adicionalmente, neste documento é discutida a adaptação da legislação Europeia sobre proteção de dados em países como a Áustria, Espanha, Portugal e República Checa.

2. RGPD

O RGPD (Regulamento (UE) 2016/679) é um regulamento da UE relativo à proteção e privacidade de dados pessoais de todos os cidadãos na UE e no Espaço Económico Europeu (EEE). Paralelamente, este regulamento aborda ainda a utilização de dados pessoais para áreas geográficas não abrangidas pelos espaços mencionados anteriormente. O RGPD entrou em vigor em maio de 2018 e apresenta três grandes objetivos:

a) **Harmonizar a legislação de proteção de dados** na Europa;

b) **Proteger e fortalecer a privacidade de dados de cada cidadão da UE;**

c) **Reorganizar a abordagem das organizações relativamente à privacidade de dados.**

Figura 1 - RDPD

Fonte: Adaptado de Business2Community (2019)

Com o RGPD, a Europa afirma a sua posição em relação à privacidade e segurança dos dados uma vez que o RGPD obriga as empresas/organizações a reorganizarem-se no que respeita à gestão e tratamento de dados. O RGPD aplica-se assim a:

a) **Empresas ou entidades residentes no território europeu que realizem tratamento de dados pessoais como uma das suas atividades de negócio**; ou,

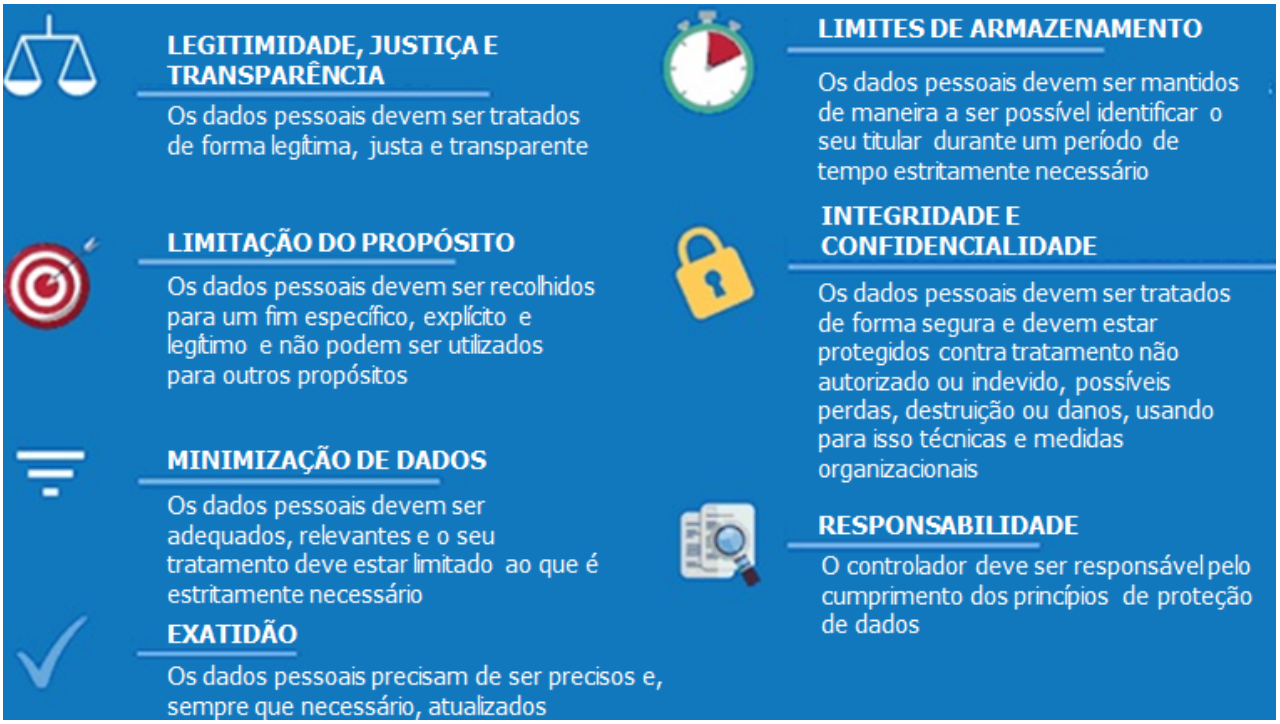
b) **Empresas ou entidades estabelecidas fora da UE que disponibilizem produtos/serviços** (pagos ou gratuitos) ou que monitorizem o comportamento de indivíduos na UE.

2.1. Princípios do RGPD

O RGPD apresenta vários princípios gerais referentes ao tratamento de dados pessoais. Um desses princípios dita que os dados pessoais necessitam de ser processados de forma transparente, isto é, o processamento dos dados pessoais deve ser claro e legítimo. Além disso, a quantidade de dados processados deve ser a menor possível; a informação deve ser precisa; e, o tempo de armazenamento desses dados deve estar limitado a um período de tempo definido, tendo em conta o seu propósito final. Paralelamente, deve estar assegurada a integridade e confidencialidade dos dados.

Os principais objetivos do RGPD encontram-se representados na figura seguinte.

Figura 2 - Princípios do RGPD



Fonte: Adaptado de I-scoop (2019)

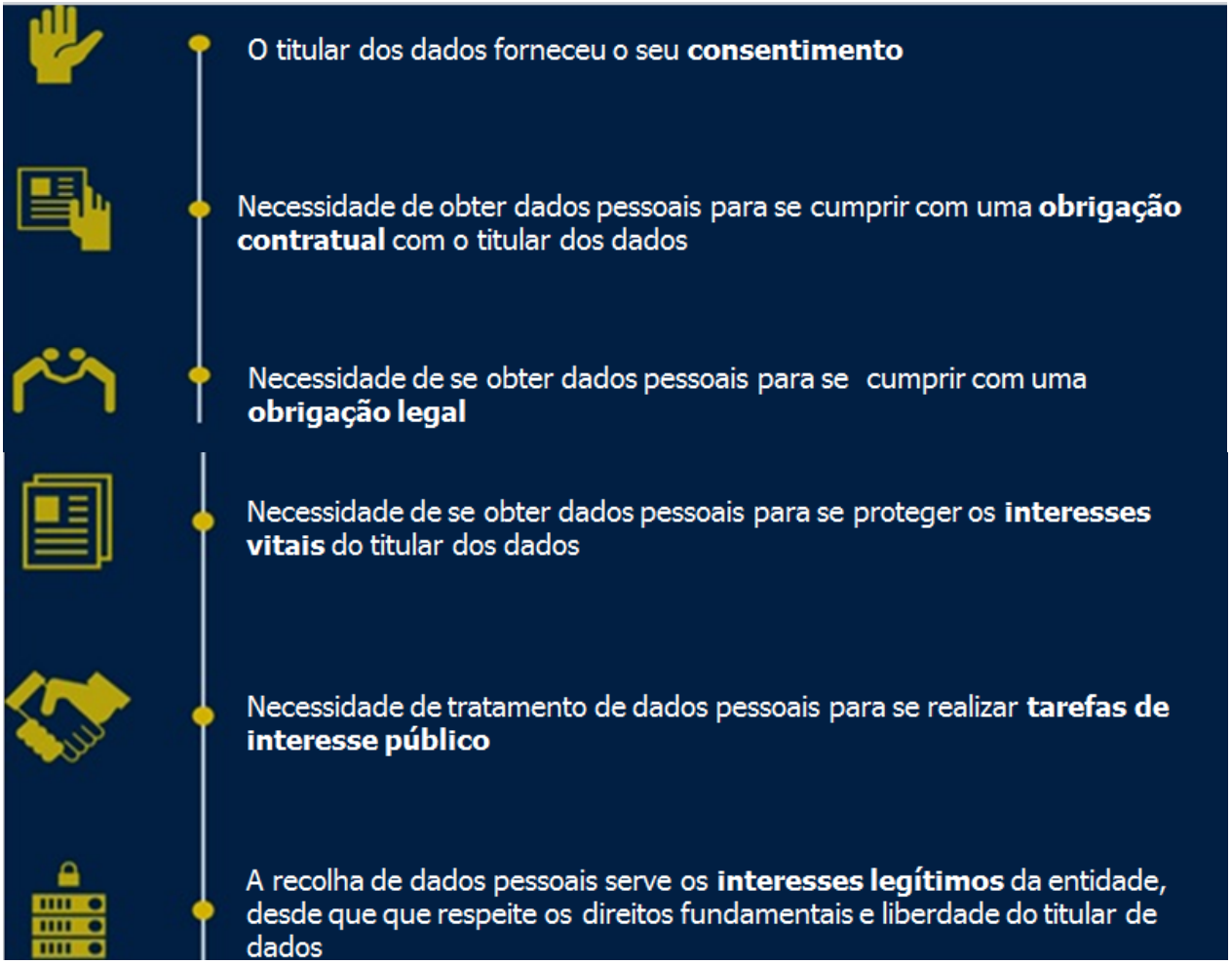
De uma forma geral, cada membro da UE dispõe de um Data Protection Act (DPA), onde cada empresa/organização sediada nesse país pode consultar as obrigações nacionais referentes à proteção de dados. No entanto, se a empresa/organização utiliza dados de diferentes estados-membros da UE, ou se se encontra inserida num grupo de diversas organizações sediadas em diferentes estados-membros, poderá ser necessário ter de consultar o DPA referente aos restantes estados-membro da UE.

Consulte a Autoridade Nacional de Proteção de Dados de cada estado-membro da UE em:
https://edpb.europa.eu/about-edpb/board/members_pt

2.2. Utilização, tratamento, armazenamento e transferência de dados na UE

O utilizador - seja um indivíduo, empresa ou organização - tem o direito de utilizar, recolher, armazenar, transferir ou gerir dados pessoais, assim como tem o direito de utilizar uma base de dados ou serviços de armazenamento em nuvem, em qualquer lugar da UE. As normas referentes aos dados pessoais diferem das normas referentes aos dados não-pessoais. No entanto, regra geral, os dados pessoais e não pessoais são recolhidos e armazenados em conjunto - este fenómeno é conhecido como mistura de dados. Aquando o tratamento dos dados pessoais, as empresas/organizações necessitam de cumprir com certos requisitos sendo que os mesmos encontram-se brevemente representados na próxima figura.

Figura 3 - Tratamento dos dados pessoais



Fonte: Adaptado de Comissão Europeia (2019)

Durante o tratamento de dados, os dados pessoais podem migrar entre diferentes empresas ou organizações. Neste ciclo de transferência de dados existem dois principais perfis de utilizador que lidam com o tratamento de dados pessoais: o controlador de dados e o processador de dados.

Figura 4 - Controlador de dados e processador de dados

Controlador de dados: decide o objetivo e o método de tratamento dos dados pessoais

Processador de dados: retém e processa os dados em nome do controlador de dados

Fonte: Elaboração própria

As empresas/organizações que processam dados são obrigadas a manter registos das atividades de tratamentos, salvo se tiverem menos de 250 trabalhadores. As demais, empresas/organizações necessitam de designar um Data Protection Officer (DPO), isto é, um responsável pela proteção de dados quando se verifica pelo menos uma das seguintes condições:

- Quando o tratamento é realizado por um organismo público (exceto tribunais);
- Quando a atividade de negócio da empresa envolve atividades como o processamento de informação e a monitorização regular de informação de cariz pessoal em grande escala;
- Quando são tratadas categorias especiais de dados ou "dados relacionados com infrações e condenações criminais".

O DPO pode ser selecionado pela organização e é responsável por monitorizar o processo de tratamento de dados pessoais, assim como por informar e aconselhar os trabalhadores que têm acesso aos dados pessoais sobre as suas obrigações. O DPO pode ser um trabalhador da organização ou pode ser uma pessoa contratada

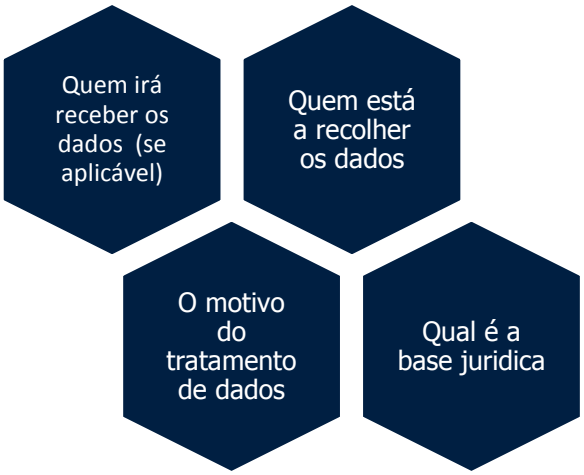
externamente, através da celebração de um contrato de serviço. Para além disso, o DPO colabora com a Autoridade de Proteção de Dados (APD) servindo como elo de ligação entre a APD e os cidadãos.

2.3. Consentimento de tratamento de dados

A responsabilidade de cumprir com o RGPD depende das entidades/organizações que processam os dados pessoais. Considerando a natureza, o âmbito, o contexto e os objetivos do tratamento de dados pessoais, para além de considerar rigorosamente os direitos e a liberdade dos cidadãos, o controlador deverá implementar técnicas e medidas organizacionais apropriadas, de maneira a garantir que o tratamento dos dados é efetuado de acordo com este regulamento. Se necessário, estas medidas deverão ser revistas e atualizadas. Alguns exemplos destas medidas são a criação de pseudónimos e a criptografia.

O RGPD aplica regras rígidas para o tratamento de dados efetuado através de consentimento prévio sendo que o objetivo destas regras é garantir que o indivíduo compreende o que está a consentir. Isto significa que o consentimento deve ser dado livremente através de um ato afirmativo, como por exemplo assinalar uma caixa de seleção ou assinando um formulário. Quando alguém consente o tratamento dos seus dados pessoais, os dados apenas podem ser utilizados para o fim mencionado no consentimento. De notar que se deve fornecer informação relativa à razão da recolha e tratamento de dados, assim como informação sobre o responsável pelo tratamento dos mesmos. A figura abaixo apresenta o mínimo de informação a ser fornecida:

Figura 5 - Tratamento de dados pessoais



Fonte: Adaptado de Comissão Europeia (2019)

Em algumas situações, a informação a ser fornecida também deve conter:

- Contacto do DPO (se aplicável);
- O interesse legítimo da empresa, sempre que se justificar a necessidade de avaliar esta situação no tratamento de dados;
- Os procedimentos e medidas aplicadas para a transferência de dados para um país fora da EU;
- Por quanto tempo serão armazenados os dados pessoais;
- Os direitos do indivíduo na proteção de dados;
- Como se procede à revogação do consentimento do tratamento de dados pessoais (quando o consentimento representa a base legal do tratamento de dados);
- Se existe, ou não, uma obrigação legal ou contractual para se ceder os dados;
- No caso de decisões automatizadas, também é obrigatório fornecer informação sobre a lógica, o alcance e as consequências da decisão.

De referir que esta informação deve ser simples, clara e explícita.

As condições para o consentimento do tratamento de dados foram reforçadas e as empresas/organizações já não podem utilizar termos ilegíveis e cláusulas repletas de

conceitos técnicos legais. O pedido para o consentimento deve ser efetuado de forma compreensível através de um formulário de acesso fácil, com o propósito da recolha de dados anexada ao formulário de consentimento. O consentimento informado deve ser facilmente distinguível de outros formulários e devem utilizar uma linguagem compreensiva e acessível.

A próxima figura demonstra um exemplo do procedimento que deve ser seguido. De igual modo, na figura pode-se observar que o RGPD alterou vários hábitos/comportamentos das empresas/organizações. Consequentemente, as empresas necessitam de rever as suas práticas internas, por exemplo, os formulários e requerimentos necessitam de ser reformulados para ficarem adaptáveis para correio eletrónico por exemplo. De maneira a receberem informação de comunicação, os interessados devem preencher um formulário ou assinalar uma caixa de seleção, confirmando posteriormente as suas intenções por e-mail.

Figura 6 - Exemplo de consentimento informado

Fonte: Adaptado de SuperOffice (2019)

2.4. Direito ao acesso e portabilidade de dados

As empresas e organizações devem assegurar que os indivíduos têm o direito de acederem aos seus dados pessoais sem qualquer tipo de custo. Se a empresa/organização receber um pedido desta natureza, deverão fazer o seguinte:

- Informar o requerente se os seus dados pessoais em questão estão a ser tratados;
- Informar o requerente sobre as especificidades relacionadas com o tratamento de dados (finalidade do tratamento, categorias de dados pessoais em causa, etc);
- Disponibilizar uma cópia dos dados pessoais que estão a ser tratados (através de formato acessível).

Com o novo RGPD, torna-se importante informar o cliente ou o titular dos dados pessoais sobre o que acontece à informação. Os direitos que necessitam de atenção especial estão sintetizados na próxima figura.

Figura 7 - Direitos contemplados no RGPD

Fonte: Adaptado de Serveit (2019)

Estes direitos são atribuídos aos indivíduos para protegerem a sua vida privada e controlar a sua pegada digital que surge através do uso de serviços e aplicações na internet. Com estes direitos pretende-se criar abertura, controlo e confiança entre todas as partes envolvidas.

2.5. Violação de dados

A violação de dados ocorre quando são divulgadas informações sobre os dados pessoais, acidentalmente ou por má-fé, a destinatários não autorizados, quando essa informação fica temporariamente indisponível ou quando é alterada.

No caso de se verificar a ocorrência de uma violação dos dados que represente um risco aos direitos e à liberdade do indivíduo, a empresa/organização deve notificar a APD respetiva, num prazo de 72h após ter conhecimento da violação de dados.

2.6. Multas

As multas estão a tornar-se mais avultadas e os prazos para pagamento de infrações cada vez mais curtos. De acordo com o RGPD, as notificações de violação de dados passam a ser obrigatórias em todos os estados membros da EU sempre que se verifica que essa violação de dados poderá representar um risco aos direitos e à liberdade do indivíduo. Após se verificar a violação de dados, a notificação deverá ser efetuada num prazo de 72h. Nestas situações, o responsável pelo tratamento dos dados pessoais deverá notificar os clientes e a própria APD após terem tido conhecimento da violação de dados pessoais. Consequentemente, o RGPD introduz um processo de execução mais rígido que obriga as entidades a terem uma maior responsabilidade financeira. Neste momento, encontram-se em análise vários casos mediáticos de violação de dados sendo que a aplicação de multas pode atingir os 4% dos rendimentos anuais da empresa, caso se verifique uma infração grave. A sanção máxima aplicável são 20 milhões de euros ou 4% dos rendimentos anuais, consoante o montante mais elevado. As autoridades de proteção de dados também podem emitir outro tipo de penalizações não financeiras tais como a proibição do tratamento de dados ou reprimendas públicas.

Segundo o RGPD, as multas são emitidas pelo regulador de proteção de dados de cada

país da UE. O montante final das multas será calculado tendo em conta os seguintes parâmetros: gravidade e natureza; intenção; mitigação, medidas de precaução; historial, cooperação; categoria dos dados; notificação; certificação; e, fatores agravantes/atenuantes. Se os reguladores determinarem que uma organização possui múltiplas violações ao RGPD a empresa terá uma penalização mais grave, desde que todas as infrações integrem o mesmo processo operativo.

2.7. Preparação para cumprimento do RGPD

O RGPD impõe certos requisitos intransigentes sobre a forma como as empresas coletam, armazenam e gerem os dados pessoais. Tendo isso em consideração, o RGPD permite que os cidadãos da UE detenham um maior controlo sobre os seus dados pessoais, assegurando que a sua informação pessoal está segura e a ser protegida por toda a Europa, independentemente de os dados serem processados dentro ou fora da UE.

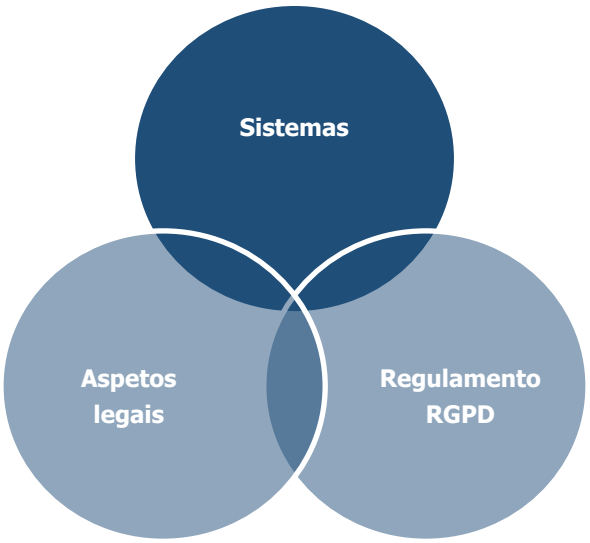
O RGPD compreende três grandes áreas que todos os negócios necessitam de considerar (ver figura 5):

1. O próprio regulamento do **RGPD**;

2. Os **sistemas** que as entidades utilizam para armazenar os dados dos seus clientes;

3. Os **aspetos legais** do regulamento e como estes afetam a forma de tratar os dados pessoais.

Figura 8 - Cumprimento do RGPD



Fonte: Elaboração própria

Adicionalmente, um aspeto crucial da legislação do RGPD diz respeito à privacidade de dados desde a sua conceção. A privacidade de dados desde a sua conceção exige que todos os departamentos dentro de uma empresa/organização analisem e sejam críticos relativamente à forma como utilizam a informação que têm disponível. Existem vários tópicos que as entidades têm de analisar e cumprir de forma a estarem em conformidade com o RGPD. Na lista que se segue encontram-se alguns passos que as empresas/organizações podem seguir aquando da implementação do RGPD:

1. **Sistematizar os dados pessoais da empresa:** sistematizar de onde provêm os dados pessoais detidos pela empresa e registar tudo que se faz com essa mesma informação. Além disso, também é importante identificar onde se encontram armazenados os dados, quem pode aceder aos mesmos e quais os riscos associados;

2. **Determinar quais são os dados necessários que é preciso manter:** o RGPD incentiva um tratamento mais disciplinado dos dados. Por este motivo, é

crucial manter apenas a informação estritamente necessária, removendo qualquer informação pessoal que não esteja a ser utilizada. Se a empresa/organização estiver a recolher uma grande quantidade de dados sem qualquer tipo de benefício/uso, deve considerar qual a informação importante e necessária para a entidade e excluir a restante. Durante o "processo de limpeza", a empresa/organização pode ter como linha orientadora as seguintes questões:

- Por que razão estamos a arquivar/armazenar estes dados/informação?;
- Qual é o nosso objetivo com a recolha de categorias de dados pessoais?;
- O ganho financeiro será superior com a eliminação da informação em comparação com a encriptação de dados?.

3. **Implementar medidas de segurança:** desenvolver e implementar medidas de segurança ao longo das infraestruturas ajuda a prevenir eventuais fugas de informação que podem resultar numa situação de violação de dados. Caso se verifique uma violação de dados é necessário aplicar medidas de segurança contra a violação de dados e agir rapidamente no caso de existir uma notificação, por parte dos indivíduos e autoridades, no caso de ocorrer uma violação de dados;

4. **Rever a documentação existente:** segundo o RGPD, os indivíduos necessitam de consentir de forma explícita a aquisição e tratamento dos seus dados pessoais. Para este efeito, as caixas de seleção previamente selecionadas e um consentimento implícito não serão aceites.

2.8. Sensibilização do RGPD - um ano após implementação

Após um ano de implementação do RGPD - a mais importante e significativa mudança no que respeita ao enquadramento legal de proteção de dados - os cidadãos europeus estão mais cada vez mais conscientes sobre os seus direitos e deveres relativamente à proteção de dados pessoais.

De acordo com os resultados do relatório "Regulamento Geral de Proteção de Dados", elaborado pela Comissão Europeia e publicado em junho de 2019, a maioria (mais de dois terços) dos europeus já ouviram falar do RGPD, assim como já ouviram falar sobre os direitos garantidos pelo RGPD, com a exceção do direito de opinião em casos onde as decisões são automatizadas (41%). Adicionalmente, o mesmo estudo refere que os países com mais conhecimentos acerca do RGPD são: a Suécia (90%); os Países Baixos (87%); e, a Polónia (86%). Além disso, os inquiridos com idades compreendidas entre os 25-54 anos (75%) são os mais ouviram falar sobre o RGPD, os inquiridos com idade entre os 15-54 conhecem melhor os seus direitos de proteção de dados comparativamente aos inquiridos com idade superior a 55 anos e os homens, comparativamente às mulheres, têm maior probabilidade de conhecerem quais são esses direitos. Quanto maior as habilitações literárias dos inquiridos, maior a probabilidade de conhecerem a legislação aplicável.

A Irlanda, a Eslováquia e a Polónia são os países que apresentam uma maior percentagem de respondentes que já ouviram falar e conhecem o RGPD e que se mostraram conhecedores de todos os direitos mencionados no questionário do estudo referido anteriormente.

No que diz respeito ao conhecimento acerca da existência de uma APD, a maioria dos inquiridos (6 em 10) indicam que já ouviram falar da existência de uma entidade pública no seu país responsável pela proteção dos seus dados pessoais.

Desde 2018, as APD nacionais são responsáveis pela imposição destas regras, verificando-se uma melhoria na coordenação das suas atividades. No entanto, ainda existe algum trabalho a ser feito relativamente a questões de conformidade, uma vez que se trata de um processo dinâmico.

De acordo com o relatório legal Deloitte "O RGPD: Seis meses após implementação:

Perspetivas e desenvolvimentos" ainda há algum trabalho a ser desenvolvido relacionado com a implementação do RGPD. As conclusões mais importantes deste relatório indicam que é importante:

- No que toca ao tratamento de dados pessoais, a primeira tarefa a realizar é conhecer os detalhes do próprio processo em si, uma vez que existe uma falta de conhecimento sobre as regras básicas;
- Melhorar a transparência sobre o tratamento de dados pessoais, informando os titulares dos dados, tal como é exigido no RGPD;
- Melhorar a orientação, recomendações ou posições oficiais da autoridade de controlo de proteção de dados daquele país;
- Conduzir formações de sensibilização junto das equipas de trabalho, incentivando todas as pessoas a informarem-se sobre os requisitos mais relevantes do RGPD, uma vez que toda a gente necessita de compreender como aplicar o RGPD nas suas tarefas profissionais no seu dia-a-dia;
- A introdução de medidas de segurança que ultrapassem os requisitos mínimos que se encontram estandardizados (por exemplo, a encriptação de todos os documentos anexados a um e-mail);
- Criar uma plataforma não-comercial com o objetivo de se partilhar conhecimento legal especializado, boas práticas e soluções criativas e práticas entre os especialistas de proteção de dados pessoais;
- Criar diretrizes direcionadas para pequenas e médias empresas, de forma a auxiliá-las na aplicação prática do novo regulamento legal de proteção de dados;
- Criar diversas *templates* que descrevam o procedimento a seguir relativamente a vários aspetos do RGPD (como recolher, implementar e transferir dados pessoais e como requerer autorização para transferência de dados pessoais);
- Desenvolver iniciativas e materiais de apoio direcionadas às escolas, direcionadas a alunos de todas as idades.

3. *ePrivacy*

A estratégia do Mercado Digital Único tem como principal objetivo aumentar a confiança e a segurança dos cidadãos face aos serviços digitais. A reforma do enquadramento de proteção de dados, em particular com a adoção do RGPD, representa uma ação fundamental para se atingir este objetivo. Do mesmo modo, a estratégia do Mercado Digital Único anunciou a revisão da Diretiva 2002/58/CE (Diretiva *ePrivacy*), que está relacionada com a privacidade e as comunicações eletrónicas, tem como propósito providenciar níveis de proteção elevados relativamente à privacidade dos utilizadores de serviços de comunicação eletrónicos.

O *ePrivacy* (ePR) apresenta ainda algumas regras que garantem a proteção de privacidade no setor de comunicações eletrónicas. A título de exemplo, as comunicações eletrónicas incluem o envio de e-mails; aplicações; telefonemas; mensagens instantâneas; *spam*; marketing direto; empresas de telecomunicações, programadores de aplicações móveis; redes de publicidade móveis; entre outros. Esta diretiva fornece assim proteção contra comunicações não-solicitadas aos utilizadores e subscritores de comunicações eletrónicas.

O ePR requer que os fornecedores de serviços de comunicações eletrónicas, tais como o acesso à internet e telefone móvel e fixo:

a) Adotem medidas de segurança para os serviços de comunicação eletrónica;

b) Garantam a confidencialidade das comunicações e tráfego de dados em redes públicas.

Os **três principais objetivos do ePR** são:

- Assegurar, por toda a UE, um nível equivalente de proteção dos direitos fundamentais ligados à privacidade e à confidencialidade, no que diz respeito ao tratamento de dados pessoais no setor das comunicações eletrónicas. Esta proteção estende-se aos subscritores que neste caso são as entidades legais;
- Garantir o direito fundamental de proteção de dados no que diz respeito ao tratamento de dados pessoais no setor das comunicações eletrónicas;

- Garantir o livre movimento de dados pessoais tratados no setor das comunicações eletrónicas e o livre movimento de serviços e equipamentos terminais de telecomunicações por toda a UE.

O ePR irá substituir a atual Diretiva Europeia *ePrivacy* e a Diretiva de Comunicações Eletrónicas de 2002. Este regulamento é assim bastante importante pois irá ser um regulamento legal que estará em vigor em todos os estados-membros, tal como acontece com o RGPD. Para além disso, esta proposta deve estar coerente com o RGPD.

Enquanto o RGPD garante a proteção dos dados pessoais, o ePR tem como principal objetivo garantir o sigilo das comunicações que poderão conter dados não-pessoais e dados relativos a uma empresa.

A entrada em vigor do ePR estava prevista para o dia 25 de maio de 2018, juntamente com o RGPD no entanto, devido a uma contínua deliberação e algum *lobbying*, a aplicação deste regulamento sofreu alguns atrasos.

3.1. Pontos principais da proposta da Comissão Europeia

A proposta para uma regulamentação de privacidade a alto nível, para todas as comunicações eletrónicas inclui:

Figura 9 - Regras do *ePrivacy*

Conteúdo das comunicações e metadados: é assegurada a privacidade dos conteúdos das comunicações e dos metadados, como por exemplo, a localização e o tempo de duração de uma chamada telefónica. Os metadados têm uma forte componente de proteção de privacidade e necessitam de ser eliminados se o titular de dados não fornecer o seu consentimento, exceto quando são utilizados para efeitos de faturação

Novos serviços: o EPR abrange a aplicação de regras de privacidade aos novos serviços de comunicação baseados na internet (p.e. *WhatsApp, Facebook Messenger* e *Skype).* Tal assegura que este tipo de serviços garantam o mesmo nível de segurança de comunicações que os serviços tradicionais de telecomunicação

Regras mais rígidas: a proteção das telecomunicações abrange as pessoas individuais e coletivas na UE. No caso de pessoas coletivas, as regras serão comuns para toda a UE

Novas oportunidades de negócio: após o titular de dados fornecer o consentimento dos seus dados pessoais haverá mais oportunidades para os prestadores de serviços de telecomunicações, fornecendo serviços adicionais e desenvolvendo o seu negócio

Regras facilitadas para os *cookies*: a aceitação das políticas *cookies*, que resultou num excesso de pedidos de consentimento por parte dos utilizadores, irá ser simplificada. Estas novas regras tornarão as plataformas de internet mais fáceis de utilizar. Do mesmo modo, não é necessário dar consentimento às políticas cookies quando estas não utilizam informação privada

Proteção contra *spam:* esta proposta proibe a existência de comunicações eletrónicas não solicitadas através de e-mail, SMS ou máquinas de chamadas automáticas. Dependendo da lei nacional, as pessoas são automaticamente protegidas ou poderão optar por não receber chamadas de marketing. As comunicações de marketing devem exibir um número identificável ou apresentar um código específico que indique que se trata de uma chamada de marketing

Execução efetiva: a APD será responsável pelo controlo e execução do regulamento, tal como acontece com o RGPD

Fonte: Adaptado de Comissão Europeia (2019)

3.2. Regras de privacidade mais rigorosas para comunicações eletrónicas

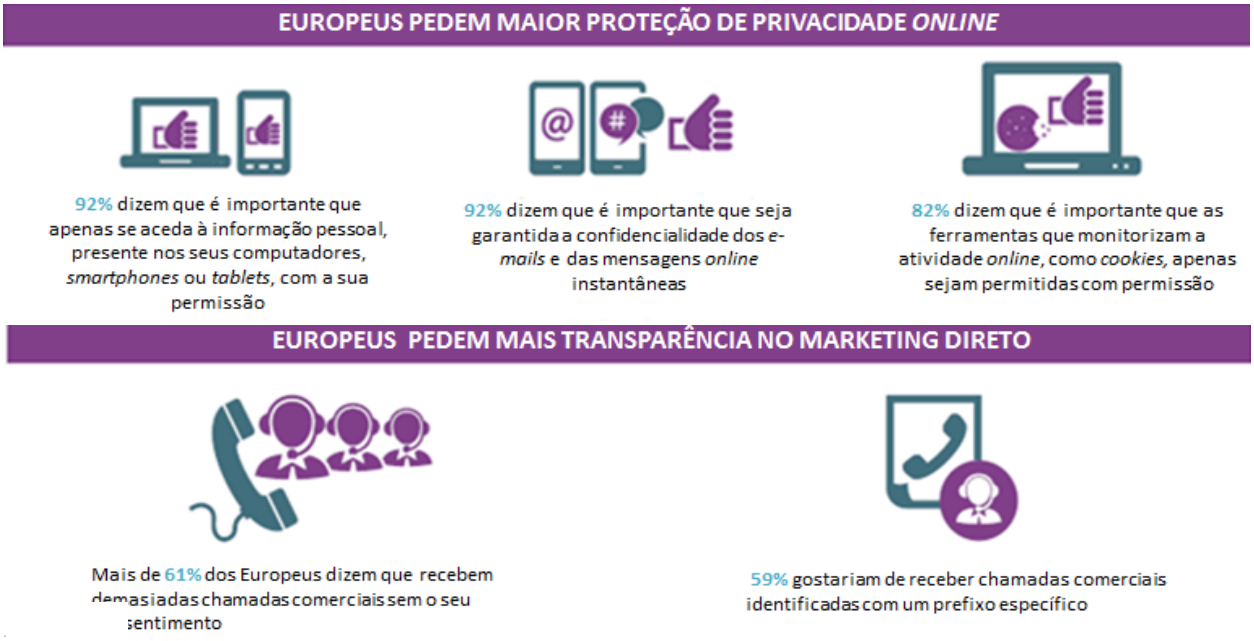
Como mencionado anteriormente, cada vez mais europeus utilizam serviços de comunicação *online* e, com o ePR, as comunicações eletrónicas dentro da UE são confidenciais, independentemente da tecnologia utilizada. As regras propostas aplicam-se também a serviços de voz e mensagem baseadas na internet.

Na figura seguinte, é possível observar que os europeus necessitam de uma proteção de privacidade mais rigorosa, especialmente nos seus dispositivos móveis (que incluem o computador, *smartphone* e *tablet*).

Adicionalmente, os europeus estão a exigir uma maior transparência no que respeita aos serviços ligados ao marketing direto. Por esta razão, com este regulamento, as pessoas terão de dar o seu consentimento antes de receberem mensagens de marketing automáticas, efetuadas através de, por exemplo, aparelhos de chamadas automáticas, SMS ou correio eletrónico. De igual modo, os cidadãos terão também de dar o seu consentimento para receber chamadas de marketing, exceto se a lei nacional permitir que o indivíduo tenha direito de se opor à receção de tais chamadas. Adicionalmente, o autor da chamada de marketing terá de garantir que o seu número

de telefone aparece visível no visor do telemóvel ou, em alternativa, terá de utilizar um prefixo especial que indique que se trata de uma chamada de marketing.

Figura 10 - Proteção de privacidade *online*



Fonte: Adaptado de Comissão Europeia (2017)

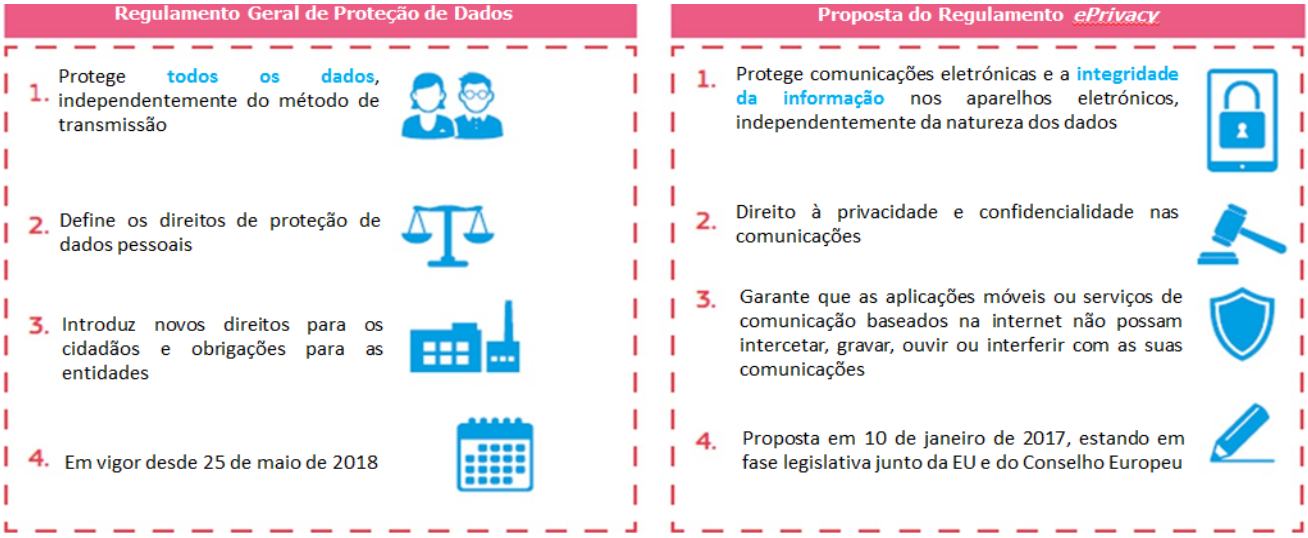
3.3. Lei aplicável e situações transfronteiriças

A diretiva *ePrivacy* não contém disposições explícitas sobre a lei nacional aplicável o que pode originar alguma incerteza sobre qual a lei que impera num contexto transfronteiriço. A falta de clareza nestas situações surge devido à inexistência de uma lei específica e comum que impede uma aplicação concreta das leis numa situação além-fronteiras.

3.4. Relação entre o RGPD e o ePR

Existem algumas diferenças e semelhanças entre o RGPD e o ePR. Enquanto o ePR protege a confidencialidade das comunicações eletrónicas o RGPD protege os dados pessoais. Isto significa que o ePR complementa o RGPD no âmbito das comunicações eletrónicas. Na figura que se segue apresenta-se uma comparação entre o RGPD e o ePR.

Figura 11 - RGPD *vs* ePR



Fonte: Adaptado de Comissão Europeia (2016)

3.5. Benefícios para os cidadãos e empresas

De acordo com a Comissão Europeia, este regulamento apresenta alguns benefícios tanto para os cidadãos como para as empresas. As principais vantagens estão contempladas na próxima figura.

Figura 12 - Benefícios para os cidadãos e para as entidades

Fonte: Adaptado de Comissão Europeia (2017)

4. Proteção de dados pessoais

De acordo com a Comissão Europeia, os dados pessoais dizem respeito a informações relacionadas com um indivíduo vivo, identificado ou passível de ser identificado, isto é, os dados pessoais são todas as informações que podem ser utilizadas para identificar um determinado indivíduo.

A UE apresenta dois principais regulamentos relacionados com a proteção e a privacidade dos dados pessoais: o RGPD e o ePR. O RGPD 2016/679 é um regulamento que está relacionado com a proteção e a privacidade de dados pessoais para todos os cidadãos da UE e do Espaço Económico Europeu (EEE). O RGPD entrou em vigor no dia 25 de maio de 2018 em todos os países europeus e tem como objetivo principal criar uma lei uniforme sobre segurança dos dados pessoais de maneira a que cada país membro da UE não necessite de desenvolver e implementar a sua própria lei de proteção de dados, fazendo com que, consequentemente, as leis se tornem consistentes por todos os países pertencentes à UE. Os requisitos do RGPD pretendem criar assim uma base legal uniforme para todos os países dentro da EU no que respeita à proteção dos dados pessoais.

Adicionalmente, o RGPD foca-se em garantir que os utilizadores entendem, compreendem e consentem a recolha dos seus dados pessoais. O RGPD protege os dados pessoais independentemente da tecnologia utilizada (automática ou manual) para o tratamento de dados, de acordo com critérios pré-definidos. Do mesmo modo, é indiferente a forma de armazenamento de dados (seja em vídeo, papel, etc), pois, em todos os casos, os dados pessoais estão sujeitos a requisitos de proteção impostos pelo RGPD e pelo ePR.

O ePR foi proposto pela Comissão Europeia em janeiro de 2017, como parte da estratégia de Mercado Único Digital, revogando assim a Diretiva 2002/58/CE, e tem como principal objetivo proporcionar um alto nível de proteção da privacidade dos utilizadores de serviços de comunicações eletrónicas.

Apesar de o RGPD ser diretamente aplicável em cada estado membro da UE este apresenta algumas cláusulas abertas que proporcionam alguma liberdade aos

legisladores nacionais. Estes aspetos serão desenvolvidos na próxima secção.

4.1. Regulamentos complementares ao regulamento da EU

4.1.1. Áustria

Os regulamentos referentes à proteção de dados pessoais são:

- **RGPD** - **em alemão *Datenschutz-Grundverordung* (DSVGO**);

- ePR;

- Regulamento de Proteção de Dados Austríaco *Datenschutzgesetz* (DSG), que complementa o RGPD;

- Lei de Adaptação de Proteção de Dados 2018 (Data Protection Adaptation Act 2018) e Lei de Desregulamentação de Proteção de Dados 2018 (Data Protection Deregulation Act 2018) (duas emendas à Lei de Proteção de Dados que foram adotadas de maneira a dar resposta às cláusulas em aberto do regulamento). A Lei de Adaptação de Proteção de Dados 2018 e a Lei de Desregulamentação de Proteção de Dados foram publicadas em BGBl I nº. 120/2017 e BGBl I nº. 24/2018, respetivamente, sendo que ambas entraram em vigor em 25 de maio de 2018;

- **Diretiva de Proteção de Dados** é uma diretiva para a área da justiça e assuntos internos que se baseia na diretiva Europeia 2016/680 do Parlamento Europeu e do Conselho da UE, de 27 de abril de 2016, revogando a decisão-quadro do Conselho 2008/977/JHA (*Österreichische Datenschutzbehörde*, 2019). Esta diretiva tem como propósito a proteção dos indivíduos, no que respeita ao tratamento de dados pessoais efetuado pelas autoridades competentes, em situações como prevenção; investigação; deteção ou persecução de ofensas criminais; execução de sentenças; e, movimento livre de dados.

4.1.2. Republica Checa

No caso da República Checa, a legislação em vigor é a seguinte:

- RGPD;

- ePR;

- **Resolução nº. 205** (15 março 2010) aborda questões de cibersegurança e

estabelece o Ministro do Interior da República Checa como o coordenador de assuntos de cibersegurança, tornando-o a autoridade nacional competente para esta área;

- Resolução nº. 380 (24 maio 2010) estabelece o Conselho de Coordenação Interdepartamental para a área da cibersegurança;

- Resolução nº. 564 (20 julho 2011) está relacionada com a Estratégia de Cibersegurança Checa para o período de 2011-2015;

- **Resolução nº. 781** (19 outubro 2011) estabelece a Autoridade como coordenadora dos assuntos de cibersegurança, assim como autoridade nacional para a área de cibersegurança;

- Lei da Cibersegurança (1 janeiro 2015) está diretamente relacionada com assuntos de cibersegurança;

- Decreto-lei nº. 437/2017 (8 dezembro 2017) transposta a legislação relevante da UE e regula os critérios para determinação de um operador com o objetivo de se determinar o possível impacto que a interrupção de um serviço essencial poderá ter nas atividades económicas e relacionadas com a segurança social;

- Lei nº. 181/2014 Coll (19 dezembro 2014) sobre cibersegurança e alterações de leis relacionadas foi publicada em Collection of Laws: Decree nº. 316/2014 Coll. on Security Measures, Cybersecurity Incidents and Reactive Measures ("Regulamento de Cibersegurança"); Lei nº. 317/2014 Coll. sobre a importância dos sistemas de informação e dos seus critérios de determinação; e a Portaria nº. 315/2014 Coll. nº. 15/2014 Coll. que altera a Portaria nº. 432/2010 Coll. sobre os critérios de identificação de um elemento crítico de infraestrutura;

- Decreto-lei nº. 82/2018 Coll (21 maio 2018) está relacionada com medidas de segurança, incidentes de cibersegurança, medidas reativas, requisitos para reportar incidentes de cibersegurança e eliminação de dados (Decreto de Cibersegurança).

4.1.3. Portugal

Em Portugal, o quadro legal de proteção de dados abrange:

- RGPD;

- ePR;

- ePR (29 agosto 2012), aplica-se ao tratamento de dados pessoais no contexto da prestação de serviços de comunicações eletrónicas acessíveis ao público através de redes de comunicações públicas, nomeadamente nas redes públicas de comunicações que sirvam de suporte a dispositivos de recolha de dados e de identificação. As empresas que oferecem serviços de comunicação eletrónicos acessíveis ao público devem estabelecer procedimentos internos que permitam responder aos pedidos de acesso a dados pessoais dos utilizadores apresentados pelas autoridades judiciárias competentes, em conformidade com a referida legislação especial. De acordo com esta lei, o envio de comunicações não solicitadas para fins de marketing direto estão sujeitas a consentimento prévio expresso pelo assinante, quer seja pessoa singular ou utilizador;

- **Constituição da República Portuguesa** (artigo 35) estabelece que todos os cidadãos têm o direito de aceder aos dados pessoais informatizados que lhes digam respeito, tendo o direito de conhecer a finalidade a que os mesmos se destinam, nos termos da lei. Esta lei estabelece assim que todos os cidadãos podem exigir a retificação e a atualização dos seus dados pessoais e define o conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização e garante a sua proteção, designadamente através de entidade administrativa independente;

- Lei da proteção de dados - lei 67/98 de 26 de outubro aplica-se ao sector privado e público assim como a qualquer sector de atividade. Tem como objetivo proteger o direito de reserva da vida privada, estabelecendo os direitos, deveres e responsabilidades legais dos titulares de dados durante o tratamento de dados pessoais. Do mesmo modo, esta lei estabelece princípios e obrigações que os detentores dos dados devem obedecer durante o processo de tratamento de dados. O princípio geral desta lei estabelece que o tratamento de dados pessoais deve processar-se de forma transparente e no estrito respeito pela reserva da vida privada, bem como pelos direitos, liberdades e garantias fundamentais;

- Lei 32/2008, de 18 de julho estabelece as obrigações relacionadas com a conservação de dados pessoais, direcionada a prestadores de serviços de comunicação

eletrónica. Esta lei está relacionada com a conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações;

- Lei das Comunicações Eletrónicas - lei 5/2014 de 10 de fevereiro e o ePR. Sob estas leis, no caso de ocorrer uma fuga de informação ou uma falha na segurança, os prestadores de serviços necessitam de notificar a entidade reguladora (Autoridade Reguladora Nacional ou ANACOM), a Comissão Nacional de Proteção de Dados e, em algumas circunstâncias, o subscritor do serviço e utilizador;

- Diretiva UE 2016/1148 relacionada com cibersegurança. Sob esta diretiva, foram estabelecidas medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a UE. Esta diretiva permite a extensão da obrigação de implementar medidas de segurança e de notificar falhas de segurança a outras entidades.

4.1.4. Espanha

Em Espanha, a legislação sobre proteção de dados pessoais aplicável é a seguinte:

- RGPD;

- ePR;

- Tratado de Lisboa (Carta dos Direitos Fundamentais da UE) e a Constituição Espanhola de 1978 relacionada com a proteção de dados e privacidade e que considera ambos direitos fundamentais do cidadão;

- Códigos de conduta para a proteção de dados, aprovados ainda quando os regulamentos de proteção de dados para diferentes setores regulamentados estavam em vigor;

- Regulamentos específicos para cada setor que incluem cláusulas relacionadas com a proteção de dados, uma vez que certas categorias de dados pessoais e algumas atividades de tratamento de dados podem exigir proteções específicas, tais como o tratamento de dados no setor financeiro, nas telecomunicações ou em setores relacionados com a saúde.

- Nova lei espanhola de proteção de dados (25 maio 2018) contém

regulamentação específica de proteção de dados direcionadas a diferentes áreas, que não estão expressamente incluídas no RGPD ou que estão incluídas no RGPD mas que permitem que cada estado membro introduza uma regulamentação mais detalhada. Além disso, esta lei incorpora no sistema legal espanhol uma lista de novos direitos para o cidadão relacionados com as novas tecnologias, denominados por "direitos digitais". Do mesmo modo, esta lei inclui uma adenda à Lei Eleitoral Geral espanhola, permitindo que partidos políticos possam utilizar e tratar dados pessoais para atividades eleitorais específicas;

- Lei e-Comércio 32/2002 (LSSI) e a **Lei Geral de Telecomunicações 9/2014 (GTL)** relacionadas com regulamentos específicos a diferentes setores e que podem conter cláusulas sobre proteção de dados;

- Diretiva EU 2016/680 (27 de abril de 2016) do Parlamento Europeu e Conselho da UE, de 27 de abril de 2016, referente à proteção de pessoas singulares no tratamento de dados pessoais efetuados por autoridades competentes, quando o objetivo é prevenir, investigar, detetar ou executar ofensas criminais/sanções penais, e no movimento livre desses dados, revogando a Decisão-Quadro 2008/977/JHA;

- Código de cibersegurança que reúne as regras atualizadas que afetam diretamente a cibersegurança. No entanto, é necessário desenvolver mais pormenorizadamente regulamentação sobre cibersegurança.

Na próxima tabela é possível consultar um breve sumário sobre as leis de proteção de dados em vigor na Áustria, República Checa, Portugal, e Espanha.

Tabela 1 - Legislação sobre proteção de dados pessoais

	Dados pessoais		Dados não pessoais	Legislação adicional sobre dados pessoais	Breve explicação
	RGPD	ePR	Regulamento (EU 2018/1807)		
Áustria	✓	✓	✓	**Lei de proteção de dados Austríaca *Datenschutzgesetz***	A Lei de proteção de dados Austríaca (DSG) que complementa o RGPD
				Lei de Adaptação de Proteção de Dados 2018 (BGBI I nº. 120/2017)	Estas duas leis foram adotadas para complementar as cláusulas abertas da Lei de Proteção de Dados (para além de diversas adendas a várias leis). Adicionalmente, estas leis complementam o RGPD
				Lei de Desregulamentação de Proteção de Dados 2018 (BGBI I nº. 24/2018)	
				Diretiva de proteção de Dados	Esta diretiva é baseada na Diretiva Europeia (EU) 2016/680 do Parlamento Europeu e do Conselho da UE, de 27 de abril de 2016, sobre a proteção dos indivíduos relativamente ao tratamento de dados por parte das autoridades competentes, em situações como prevenção, investigação, deteção ou persecução de ofensas criminais, execução de sentenças, no movimento livre de dados
República Checa	✓	✓	✓	**Resolução nº. 205**	Aborda problemas de cibersegurança e estabelece o ministro do Interior da República Checa como o coordenador nacional de cibersegurança, assim como a autoridade nacional para aquela área
				Resolução nº. 380	Estabelece um conselho de coordenação interdepartamental para a cibersegurança
				Resolução nº. 564	Estratégia de Cibersegurança Checa 2011-2015
				Resolução nº. 781	Autoridade como coordenadora dos assuntos de cibersegurança, assim como autoridade nacional para a área de cibersegurança

				Lei de Cibersegurança	Regulamenta a cibersegurança na República Checa, tendo entrado em vigor no dia 1 de janeiro de 2015
				Decreto nº. 437/2017	Transpõe a legislação relevante da EU e regula critérios para determinação de um operador com o objetivo de se determinar o possível impacto que a interrupção de um serviço essencial poderá ter nas atividades económicas de segurança social
				Lei nº. 181/2014 Coll	Relacionada com a cibersegurança e altera leis relacionadas com este tópico
				Decreto nº. 82/2018 Coll	Relacionada com medidas de segurança, incidentes de cibersegurança, medidas reativas, requisitos para reportar incidentes de cibersegurança e eliminação de dados (Decreto de Cibersegurança)
Portugal	✓	✓	✓	***ePrivacy***	Tratamento de dados pessoais no contexto da prestação de serviços de comunicações eletrónicas acessíveis ao público em redes de comunicações públicas, nomeadamente nas redes públicas de comunicações que sirvam de suporte a dispositivos de recolha de dados e de identificação
				Constituição da República portuguesa (artigo 35)	Estabelece que todos os cidadãos têm o direito de aceder aos dados informatizados que lhes digam respeito, podendo exigir a sua retificação e atualização e o direito de conhecer a finalidade a que se destinam, nos termos da lei. Do mesmo modo, determina o conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, e garante a sua proteção, designadamente através de entidade administrativa independente.
				Lei 67/98, de 26 de outubro	Enquadramento legal sobre proteção de dados, que se aplica ao setor público e privado, assim como qualquer a qualquer setor de atividade
				Lei 32/2008 de 18 de julho	Estabelece as obrigações relacionadas com a conservação de dados, direcionada aos prestadores de serviços de comunicação eletrónica
				Lei 5/2014 de 10 de fevereiro e *ePrivacy*	Impõem que, no caso de ocorrer uma fuga de informação ou uma falha na segurança, os prestadores de serviços necessitam de notificar a entidade reguladora, a Comissão Nacional de Proteção de Dados e, em algumas circunstâncias,

					o subscritor do serviço e utilizador
				Diretiva UE 2016/1148	Estende a obrigação de implementação de medidas de segurança e de notificação em caso de violação de dados a outras entidades
Espanha	✓	✓	✓	**Tratado de lisboa Constituição Espanhola de 1978**	Relacionadas com a privacidade e proteção de dados como direitos fundamentais
				Nova lei espanhola de proteção de dados Lei 3/2018 de 7 de dezembro	Fornece regulamentação específica para a proteção de dados em diferentes áreas que não estão expressamente incluídas no RGPD
				Lei *e-commerce* 34/2002 (LSSI) Lei Geral das Telecomunicações 9/2014 (GTL)	Regulamentação direcionada a áreas específicas
				Diretiva UE 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016	Proteção de pessoas singulares no tratamento de dados pessoais efetuados por autoridades competentes, quando o objetivo é prevenir, investigar, detetar ou executar ofensas criminais/sanções penais, e no movimento livre desses dados, revogando a Decisão-Quadro 2008/977/JHA
				Código de cibersegurança	Indica as regras principais a ter em consideração no que respeita ao ciberespaço e na execução dos métodos de cibersegurança

Fonte: Elaboração própria do autor

5. Dados não-pessoais

O livre fluxo de dados não pessoais traduz-se num movimento de dados além-fronteiras e a existência de sistemas de Tecnologias de Informação por toda a UE.

O regulamento do livre fluxo dos dados não pessoais já se encontra em vigor na UE - Regulamento (EU) 2018/1807 do Parlamento da UE e Conselho, de 14 de novembro de 2018 - e apresenta um regime para o livre fluxo de dados não pessoais por toda a UE.

Este regulamento apresenta como principal objetivo a garantia do livre fluxo, dentro da UE, de todos os dados que não sejam dados pessoais, através da implementação de regras relacionadas com requisitos de localização de dados, a disponibilização de informação a autoridades competentes e a portabilidade de dados para usuários profissionais.

Paralelamente, este regulamento também se aplica ao tratamento de dados eletrónicos, excetuando se forem dados pessoais, dentro da UE se:

- Forem fornecidos como um serviço a utilizadores que residam ou contenham um negócio na UE, independentemente de o fornecedor do serviço estar, ou não, sediado na UE;
- Pessoa coletiva a residir ou operar na UE;
- Este regulamento não se aplica a nenhuma atividade que não é abrangida pela lei da UE.

Figura 13 - Dados não pessoais

Fonte: Adaptado de Business2Community (2019)

A garantia de um livre fluxo de dados não pessoais segue os seguintes princípios em toda a UE:

- O princípio do livre fluxo de dados não pessoais elimina restrições de localização de dados injustificadas, impostas por autoridades públicas, contribuindo para um aumento do rigor e confiança;
- O princípio da disponibilização de dados para as autoridades competentes permite que os dados permaneçam acessíveis para um controlo de supervisão e regulação, inclusive em situações onde a informação é armazenada e processada além-fronteiras da UE;
- Ações para encorajar que os prestadores de serviços em nuvem desenvolvam códigos de conduta de autorregulação para que a mudança de prestador de serviços seja realizada de forma mais fácil, transferindo-se os dados para os servidores respetivos. Estas medidas devem ser implementadas até meados do ano 2020;
- Os requisitos de segurança para o armazenamento e tratamento de dados permanecem aplicáveis em situações onde as entidades armazenam e tratam os dados noutros estados membros. O mesmo se aplica quando se subcontratam

fornecedores de serviços de armazenamento em nuvem para o tratamento de dados;

- A garantia de uma correta e efetiva aplicação das novas regras do livre fluxo de dados não pessoais através da constituição de um único ponto de contacto central em cada estado-membro, de maneira a agilizar a comunicação entre os estados-membros e entre os estados-membros e a Comissão Europeia.

O **RGPD e o regulamento de livre fluxo de dados não pessoais irão complementar-se de forma a possibilitar o livre fluxo de qualquer tipo de dados** criando um espaço europeu comum para esse tipo de informação. Estes dois regulamentos estabelecem assim uma certeza jurídica para as empresas, garantindo que os dados pessoais e não pessoais circulam livremente por toda a EU.

5.1. Livre circulação de dados na UE

Os requisitos de localização de dados devem ser proibidos, exceto em situações de segurança pública, sendo que estas devem respeitar o princípio de proporcionalidade. Assim, os estados-membros devem comunicar imediatamente à Comissão Europeia qualquer projeto de lei que apresente novos requisitos relacionados com localização de dados, ou que altere algum requisito em vigor, de acordo com os procedimentos previstos no artigo 5, 6 e 7 da Diretiva (EU) 2015/1535.

Adicionalmente, o **regulamento relacionado com dados não pessoais** salvaguarda:

- O livre movimento de dados não pessoais entre fronteiras: todas as organizações devem ser capazes de armazenar e tratar dados a partir de qualquer local geográfico localizado na UE;

- A disponibilidade de dados para fins de controlo regulamentar: as autoridades públicas têm o direito a aceder aos dados, independentemente de estes estarem localizados em outro estado-membro ou de serem tratados/armazenados num sistema em nuvem;

- **Mudança de fornecedores de serviços de uma solução na nuvem** mais

facilitada para utilizadores profissionais. A Comissão Europeia incentiva que os prestadores de serviços de nuvem desenvolvam códigos de conduta de autorregulação, onde os utilizadores podem transferir os seus dados entre diferentes fornecedores ou para um ambiente informático próprio;

- **Coerência e sinergias entre sistemas de cibersegurança**, clarificando que qualquer requisito de segurança virtual em vigor permanece em vigência em situações onde o armazenamento e tratamento de dados passe a ser efetuado noutro local da UE ou em sistemas de nuvem.

Juntamente com este regulamento, o RGPD já prevê a livre circulação de dados pessoais. As cláusulas de localização de dados serão incorporadas na legislação da UE até 31 de maio de 2021, tendo um efeito legislativo em todos os estados-membros.

5.2. Portabilidade de dados

A Comissão Europeia deve encorajar e facilitar o desenvolvimento de códigos de conduta autorregulatórios, a nível europeu, de maneira a contribuir para uma economia de dados mais competitiva e baseada no princípio de transparência.

5.3. Procedimento para cooperação entre autoridades

De acordo com o artigo 7, cada estado-membro deverá designar um ponto único de contacto que terá então como função ser o ponto de contacto entre outros estados-membros e a Comissão Europeia e garantir a aplicação efetiva deste regulamento. Tal significa que cada estado-membro deverá notificar a Comissão Europeia sobre qual o seu ponto de contacto e sobre eventualmente alguma alteração que se venha a verificar.

5.4. Disponibilidade de dados às autoridades competentes

Tendo em conta o artigo 5, este regulamento não pode constituir um fator de impedimento por parte das autoridades competentes na obtenção de acesso a dados (pessoais e não pessoais) necessários para o correto funcionamento das suas funções

oficiais, em concordância com a UE e a legislação nacional existente. De acordo o artigo 7, se após a autoridade competente requerer acesso a dados de um determinado indivíduo o seu acesso for dificultado por algum motivo, as autoridades competentes podem requerer a assistência de uma autoridade competente de outro estado-membro. Esta situação ocorre se nenhum mecanismo específico de cooperação estiver contemplado na legislação europeia ou se não existir acordo internacional para intercâmbio de informação entre diferentes estados-membros.

5.5. Sanções para infrações

Este regulamento define sanções para a ocorrência de violações de dados e contempla diferentes penas para diferentes infrações (as mesmas sanções são aplicáveis para o RGPD e para o ePR). Como tal, a pena para o caso mais grave é de 10 milhões de euros ou 2% dos rendimentos anuais, aplicando o valor mais elevado.

Podem também ser aplicadas eventuais multas que dependem de diversos fatores atenuadores, tais como: escala do incidente; eventual fuga de informação; existência de um ato premeditado; e, quais as diligências de prevenção adotadas pela organização no seguimento da violação de dados.

6. Catálogo sistematizado de conteúdos

Cibersegurança: proteção de sistemas, redes informáticas e programas contra ataques digitais. Geralmente, estes ataques pretendem aceder, alterar ou destruir informação sensível, extorquir dinheiro aos utilizadores ou interromper o funcionamento normal de negócios.

Autoridades de proteção de dados: autoridades públicas independentes que supervisionam a aplicação da Lei de Proteção de Dados. Estas autoridades providenciam conselhos técnicos em questões relacionadas com proteção de dados e são responsáveis pela gestão de queixas relacionadas com o incumprimento do RGPD e de leis nacionais relevantes.

Data Protection Officer: elemento responsável por monitorizar a aplicação das regras de proteção de dados na Comissão Europeia. Por norma, esta pessoa é um colaborador da entidade, responsável por compreender e assegurar o cumprimento destas obrigações, por parte da empresa. Igualmente, o DPO assegura a aplicação interna das regras de proteção de dados, trabalhando em cooperação com o Supervisor Europeu de Proteção de Dados.

Regulamento *ePrivacy*: proposta da Comissão Europeia para fortalecer o direito à reserva da vida privada dos cidadãos da UE criando novas oportunidades de negócio.

RGPD: regulamento da UE sobre proteção de dados e privacidade, aplicável para todos os cidadãos da UE e do EEE.

Dados não pessoais: informação eletrónica que não pode ser rastreada até a um indivíduo identificável.

Dados pessoais: qualquer informação relacionada com um indivíduo que possa direta ou indiretamente identificar determinado indivíduo. Alguns exemplos de dados pessoais são: nome; fotografias; informação geográfica; *web cookies*; endereços de correio eletrónico; entre outros.

7. Conclusões

A proteção de dados e cibersegurança estão-se a tornar valores essenciais para a sociedade. Consequentemente, estas duas áreas encontram-se atualmente sujeitas a mudanças legais apesar de estarem a tornar-se cada vez mais consolidadas na UE.

Na UE, o regulamento referente aos dados pessoais difere do regulamento para os dados não pessoais. No entanto, estes dois regulamentos são iguais para todos os estados-membros da UE. O regulamento (UE) 2018/1807 aplica-se ao livre fluxo de dados não pessoais enquanto no caso do tratamento de dados pessoais o regulamento aplicável é o RGPD. Assim, com o objetivo de se criar um espaço comum de partilha de dados (pessoais e não pessoais) na UE o RGPD e o regulamento (UE) 2018/1807 atuam em simultâneo, complementando-se mutuamente.

Paralelamente, o regulamento *ePrivacy* define algumas regras relacionadas com a proteção da privacidade no setor das telecomunicações. Este regulamento aplica-se mais particularmente aos fornecedores de redes e serviços de comunicações eletrónicas sendo que, a sua implementação estava inicialmente prevista para o dia 28 de maio de 2018, juntamente com o RGPD, o que acabou por não acontecer devido às deliberações e a existência de um *lobbying* constante que adiou a sua entrada em vigor. O ePR não contém uma disposição explícita sobre a aplicação da lei nacional em cada país o que origina alguma incerteza sobre qual a lei que impera num contexto transfronteiriço. Não obstante, apesar de a regulamentação sobre a proteção de dados ser diretamente aplicável em cada estado-membro contém inúmeras cláusulas genéricas que conferem alguma liberdade legislativa à entidade nacional.

8. Referências

Business2Community (2019). *Why User Data is the Next Big Deal in Digital?.* Disponível em https://www.business2community.com/mobile-apps/why-user-data-is-the-next-big-deal-in-digital-02179282.

Deloitte (2019). *The GDPR: Six Months after Implementation*. Disponível em https://www2.deloitte.com/bg/en/pages/legal/articles/gdpr-six-months-after-implementation-2018.html.

EU GDPR.ORG (2019). *The EU General Data Protection Regulation (GDPR) is the most important change in data privacy regulation in 20 years*. Disponível em https://eugdpr.org/.

Comissão Europeia (2019). *Complete guide to GDPR compliance*. Disponível em https://gdpr.eu/.

Comissão Europeia (2019). *Data protection under GDPR*. Disponível em https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_en.htm#shortcut-3-who-monitors-how-personal-data-is-processed-within-a-company.

Comissão Europeia (2019). *Eurobarometer on ePrivacy*. Disponível em https://ec.europa.eu/digital-single-market/en/news/eurobarometer-eprivacy.

Comissão Europeia (2019). *Free flow of non-personal data*. Disponível em https://ec.europa.eu/digital-single-market/en/free-flow-non-personal-data.

Comissão Europeia (2019). *General Data Protection Regulation: one year on.* Disponível em: https://ec.europa.eu/commission/presscorner/detail/en/IP_19_2610.

Comissão Europeia (2019). *Proposal for a regulation on privacy and electronic communications*. Disponível em https://ec.europa.eu/digital-single-

market/en/news/proposal-regulation-privacy-and-electronic-communications.

i-Scoop (2019). *Data processing principles: the 9 GDPR principles relating to processing personal data*. Disponível em https://www.i-scoop.eu/gdpr/gdpr-personal-data-processing-principles/.

ITPRO (2019). *ePrivacy Regulation: What is it and how does it affect me?*. Disponível em https://www.itpro.co.uk/privacy/32712/eprivacy-regulation-what-is-it-and-how-does-it-affect-me.

Serve IT (2017). *GDPR for developers - data subject rights*. Disponível em https://www.serveit.com/gdpr-for-developers-data-subject-rights/.