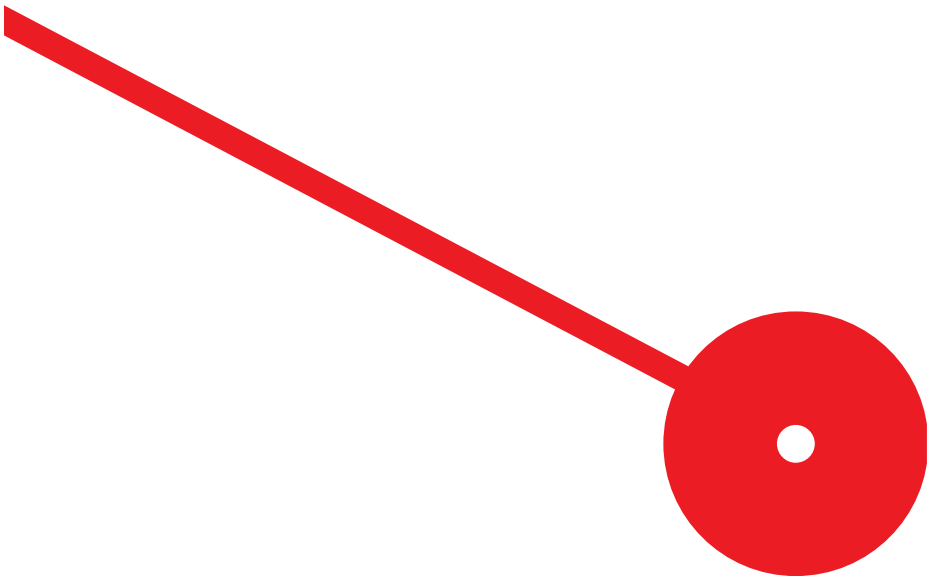
INSTITUTO
SUPERIOR
DE CONTABILIDADE
E ADMINISTRAÇÃO
DO PORTO
POLITÉCNICO
DO PORTO

M MESTRADO
ÁREA DE ESPECIALIZAÇÃO

O impacto da Proteção de Dados (RGPD) no Retalho Omnicanal

Rui Leal de Oliveira

10/2021



Rui Leal de Oliveira. O impacto da Proteção de Dados (RGPD) no Retalho Omnicanal
10/2021

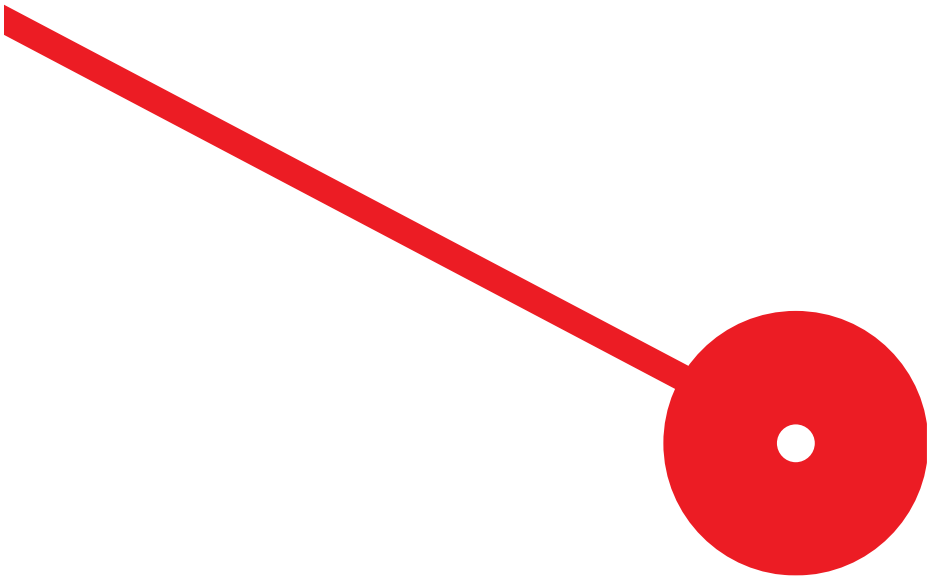
INSTITUTO
SUPERIOR
DE CONTABILIDADE
E ADMINISTRAÇÃO
DO PORTO
POLITÉCNICO
DO PORTO

M MESTRADO
ÁREA DE ESPECIALIZAÇÃO

O impacto da Proteção de Dados (RGPD) no Retalho Omnicanal

Rui Leal de Oliveira

Dissertação de Mestrado apresentado ao Instituto Superior de Contabilidade e Administração do Porto para a obtenção do grau de Mestre em Negócio Eletrónico, sob orientação do Professor Doutor Paulo Vasconcelos



Rui Leal de Oliveira. O impacto da Proteção de Dados (RGPD) no Retalho Omnicanal
10/2021

Resumo

O objetivo deste estudo é compreender de que forma o Regulamento Geral de Proteção de Dados afetou as empresas de Retalho com uma estratégia omnicanal. Este estudo investiga os impactos causados pelo Regulamento Geral de Proteção de Dados nestas entidades, as consequentes estratégias e as medidas implementadas para o incorporar. Para esta análise, esta investigação baseia-se na realização de entrevistas com representantes destas entidades em Portugal, assim como fundamentação teórica.

As conclusões do presente estudo indicam que os impactos do regulamento europeu foram, sobretudo, no processo de recolha e tratamento de dados, no processo de personalização e na partilha de dados ao longo de toda a cadeia de abastecimento. Paralelamente, além de custos de implementação, outro impacto que se destaca inclui a digitalização dos processos internos.

Palavras-Chave:

Retalho Omnicanal, Proteção de Dados, RGPD;

Abstract

The goal of this research is to understand how the General Data Protection Regulation affected retail companies with an Omnichannel strategy. The present paper approaches the impacts caused by the General Data Protection Regulation, the consequent implemented strategies and measures by these companies to incorporate it. Therefore, this paper relies on interviews to representatives of these companies in Portugal, as well as theoretical foundations.

The results of the present paper indicate that the impacts this regulation brought were, mainly, in the collection and processing procedures, in the personalization process and the data sharing inside the supply chain. Simultaneously, besides initial implementation costs, another impact that stands out is the digitalization of the companies' internal processes.

Keywords:

Omnichannel Retail, Data Protection, GDPR;

Lista de Abreviaturas, Siglas e Acrónimos

Al. - Alínea

Artº - Artigo

CE - Comissão Europeia

CNPD - Comissão Nacional de Proteção de Dados

CRP - Constituição da República Portuguesa

DPD - Diretiva da Proteção de Dados (Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995)

EPD – Encarregado de Proteção de Dados

EUA – Estados Unidos da América

LNPD – Lei Nacional de Proteção de Dados

Nº - Número

OCDE - Organização para a Cooperação e Desenvolvimento Económico

PME – Pequenas e Médias Empresas

RGPD - Regulamento Geral sobre a Proteção de Dados (Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016)

UE - União Europeia

VAB – Valor Acrescentado Bruto

Índice Geral

Índice de Figuras

Índice de Tabelas

Capítulo I - Introdução

1.1 - Enquadramento

Os últimos anos foram marcados por avanços tecnológicos sem precedentes. Desde a massificação da web, à democratização das redes sociais e, posteriormente, à captação de dados em tempo real, tudo isto permitiu o progresso do meio digital [1].

No retalho, embora o canal físico tenha dominado durante largos anos, o canal digital tem vindo a ganhar preponderância, primeiramente, devido à massificação de canais *web* e *mobile* e, agora, mais recentemente graças à pandemia do COVID-19, que obrigou governos a estabelecerem restrições à circulação e ao encerramento de lojas físicas. Face a isto, os consumidores viraram-se para o canal digital, nomeadamente, o comércio eletrônico de forma a ir ao encontro das suas necessidades. Consequentemente, os retalhistas, outrora puramente tradicionais, expandiram os seus negócios para o domínio digital [2].

Por outro lado, com o evoluir da situação pandémica, os retalhistas começaram a abrir as suas lojas físicas e a gestão e integração dos diferentes canais tornou-se fulcral para os seus negócios, potenciando o desenvolvimento de estratégias omnicanal.

No entanto, dada a sua natureza integrativa, a estratégia omnicanal, apesar dos seus benefícios, também levanta algumas questões no campo da proteção de dados, nomeadamente a recolha e tratamento de dados sem consentimento, a partilha de dados entre entidades e a dicotomia entre privacidade e personalização.

Como resposta a estas preocupações, o Parlamento Europeu, em maio de 2016, adotou o RGPD, que, por sua vez, anulou a legislação anterior, a DPD, adotada em 1995, quando a internet ainda se encontrava na sua fase embrionária. Posteriormente, os Estados-Membros procederam à implementação desta nova legislação até maio de 2018 [3].

O RGPD foi criado com o objetivo de proteger direitos fundamentais e liberdades de pessoas singulares europeias, em particular, o direito à proteção dos seus dados pessoais. Para atingir esta finalidade, o regulamento estabelece princípios fundamentais para a recolha e tratamento de dados, sendo estes: Legalidade, lealdade e transparência, Limitação das finalidades, Minimização dos Dados, Limitação do tempo de conservação, Integridade e Confidencialidade e Exatidão [4].

Desta forma, o regulamento estipula de que forma as entidades podem reunir, armazenar e utilizar dados pessoais dos seus clientes e trabalhadores. Além disso, procura devolver o controlo dos dados pessoais aos cidadãos e harmonizar as regulações para este setor dentro da União Europeia [5].

[1] (Chivot & Castro, 2019)
[2] (Deloitte China, 2020)
[3] (European Data Protection Supervisor, 2018)
[4] (Parlamento Europeu, 2016)
[5] (Ruiz, 2018)

1.2 - Objetivos da Investigação

O objetivo desta investigação pretende compreender o impacto da regulação europeia de proteção de dados pessoais nas empresas de Retalho Omnicanal em Portugal. Nesse sentido, este estudo tenciona:

- Descrever os impactos positivos da regulação europeia de proteção de dados nas empresas de Retalho Omnicanal em Portugal;
- Descrever os impactos negativos da regulação europeia de proteção de dados nas empresas de Retalho Omnicanal em Portugal;

1.3 - Questão de Investigação

Como esta investigação incide sobre o impacto da proteção de dados pessoais no retalho omnicanal em Portugal, terei que, em primeiro lugar, compreender quais foram os impactos da regulação de proteção de dados europeia. Nesse sentido, analisei os custos envolvidos necessários e as estratégias utilizadas pelas empresas para incorporar a regulação, assim como, o conteúdo das entrevistas executadas.

Recolhidos estes dados, pretende-se analisar a incidência que esta regulação teve nas estratégias das empresas e onde a regulação falha a reconhecer as necessidades das empresas.

A questão da Investigação é: ***"Que impactos o Regulamento Geral de Proteção de Dados causou nas empresas de retalho omnicanal em Portugal?"***

1.4 - Metodologia

As técnicas de investigação escolhidas para esta investigação foram a análise teórica, através de obras publicadas, artigos científicos, estudos, relatórios oficiais, casos de estudo, dissertações e revistas científicas, e a análise de entrevistas realizadas a entidades com presença omnicanal. Por último, estas empresas em Portugal que compõem a amostra são: GNG – Comércio de Vestuário SA, Grupo NOS, SGPS e Irmãos Vila Nova S.A, às quais, para os efeitos desta investigação, nos referiremos como empresa A, B e C, respetivamente.

1.5 - Organização do Trabalho

Relativamente à estrutura, o estudo organiza-se em seis distintas partes. No presente capítulo é apresentado o enquadramento do tema, os objetivos e questão de investigação, explicação da metodologia utilizada e, por fim, a forma como este estudo está organizado.

No segundo capítulo é apresentada a revisão de literatura, onde são identificadas referências teóricas que darão suporte ao estudo.

No terceiro capítulo, é demonstrada com maior detalhe a análise do RGPD e a sua transposição para Portugal.

No quarto capítulo, são analisados os impactos e as implicações do RGPD no retalho omnicanal, através dos conteúdos teóricos recolhidos e das entrevistas realizadas.

Por fim, são demonstradas as conclusões do estudo com exposição clara e concisa dos impactos.

1.6 - Trabalhos Relacionados

Existem alguns estudos que refletem diretamente os impactos do RGPD nos vários setores de atividade ou numa perspetiva macroeconómica, desde o seu impacto na confiança dos consumidores [6] até à sua aplicação nas PME portuguesas [7]. No entanto, incidindo sobretudo sobre a estratégia omnicanal, Li, Werner, Ernst & Damian levantam uma série de fatores que resultam no não-cumprimento do regulamento por parte das empresas e propõe um modelo de operacionalização e de utilização de instrumentos pró-RGPD [8]. Por outro lado, Nabbosa & Iftikhar focam-se numa análise compreensiva do RGPD e o seu impacto na jornada do consumidor, com ênfase no retalho digital [9]. Ao contrário dos anteriores mencionados, o ponto-chave desta abordagem é o levantamento dos impactos do RGPD na estratégia omnicanal, assim como a sua discriminação enquanto negativos ou positivos para as empresas portuguesas com essa estratégia implementada.

[6] (Pan & Zinkhan, 2006)
[7] (Silva, 2019)
[8] (Li, Werner, Ernst, & Damian, 2020)
[9] (Nabbosa & Iftikhar, 2019)

Capítulo II - Revisão de Literatura

No presente capítulo são apresentadas as referências teóricas que serão suporte para a realização deste estudo.

2.1 - Retalho – Conceitos Base & Jurídicos

O Retalho pode ser definido como qualquer atividade ligada à venda de bens ou serviços a um consumidor para consumo individual [10].

Juridicamente, segundo o Regulamento nº 278/2012, o retalho é designado como a atividade praticada por "*toda a pessoa física ou coletiva que, a título habitual e profissional, compra mercadorias em seu próprio nome e por sua própria conta e as revende diretamente ao consumidor*"[11]. Nesse sentido e, de acordo com o Decreto-Lei nº 339/85, o exercício do comércio a retalho pressupõe "*aquisição pelo agente, a título profissional, de mercadorias, e a direta revenda delas ao consumidor"*. Por sua vez, o conceito de Retalhista pode ser definido legalmente como aquele que exerce a atividade do *"comércio a retalho de forma fixa ou sedentária, em estabelecimentos, lojas ou instalações fixas ao solo de maneira estável em mercados cobertos" [12]*.

Com o desenvolvimento dos meios tecnológicos e de comunicação, o setor do retalho começou a expandir para a dimensão digital ou *online.* Dessa forma, podemos definir o Retalho *Online* como a realização da venda a retalho, por meios electrónicos, ao consumidor para a sua utilização pessoal e não comercial [13].

O panorama económico a nível global permanece incerto em 2021. Se por um lado, a criação e distribuição de uma vacina contra o COVID-19 ofereceu esperança a pessoas e empresas para retoma das atividades económicas, por outro, o vírus continuou a afetar a estabilidade económica. Mesmo em locais onde o surto tenha sido limitado, houve um impacto económico negativo, dadas as medidas de distanciamento social para evitar novos surtos. Para a Deloitte (2021) o sucesso das campanhas de controlo dos surtos, da proteção dos que foram afetados e a distribuição rápida das vacinas são preponderantes para determinar a trajetória da economia global para os próximos anos.

O impacto desta pandemia criou vantagens e desvantagens para os retalhistas. Numa primeira perspetiva, algumas indústrias do setor do retalho não só tiveram de enfrentar períodos de tempo com a sua atividade económica suprimida, mas também uma diminuição da mobilidade dos consumidores e um aumento da atividade *online.* No entanto, outras indústrias do setor beneficiaram desta pandemia, como por exemplo, mercearias e *e-tailers*, dado o fecho dos restaurantes e a recusa por parte dos consumidores de comprar em loja física [14].

Neste subcapitulo, caracterizamos a situação atual do setor do Retalho, a nível internacional e nacional.

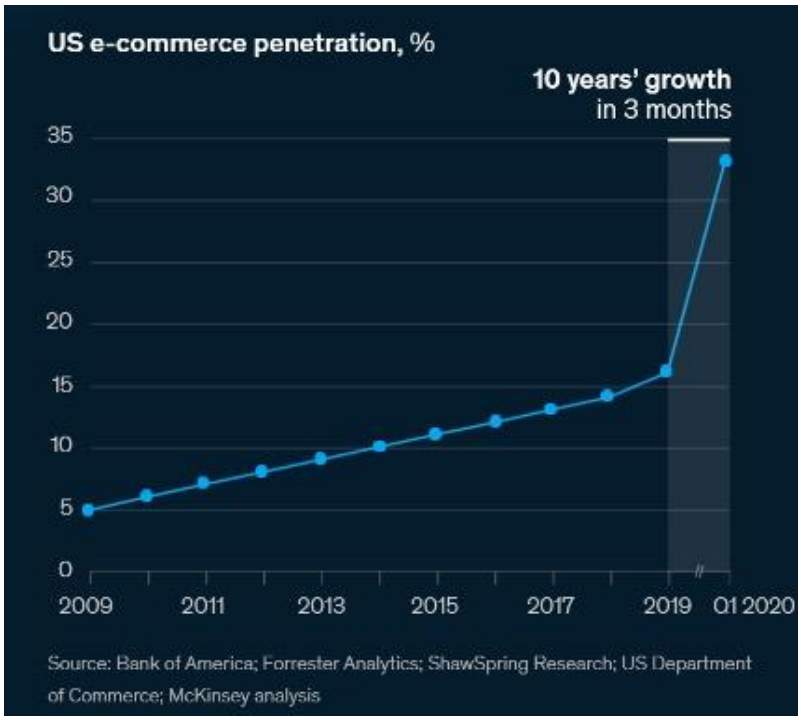
[10] (Chan, 2013)
[11] (Regulamento n.º 278/2012)
[12] (Decreto-Lei nº 339/85)
[13] (Francis & White, 2004)
[14] (Deloitte, 2021)

2.1.1 – Caracterização Atual do Setor do Retalho a nível internacional

O impacto causado pelo COVID-19 foi sentido em todos os setores da economia, especialmente o setor do Retalho. Sucessivos confinamentos, a necessária transformação digital e o foco numa experiência de compra estritamente digital pressionaram as indústrias deste setor, sobretudo no caso do retalho não-essencial. Tendo isto em conta, pode-se considerar o ano 2021, um ano desafiante e incerto para muitos retalhistas em todo o mundo.

Nos EUA, no fim do ano de 2020, a economia enfraqueceu. A redução dos rendimentos e a consequente redução do consumo levaram a uma diminuição das vendas no setor do retalho. Mesmo assim, o enfraquecimento das vendas nas lojas físicas deste setor *"foi em parte compensado por um aumento acentuado nas compras online"* [15].

Figura 1 - O "salto" do e-Commerce nos EUA entre 2009 e 2020



Fonte: (McKinsey, 2020)

Contudo, em termos percentuais, o retalho online norte-americano representa apenas 15% do total de vendas de retalho, em 2021, tal como podemos observar na figura 2.

[15] (Deloitte, 2021)

Figura 2 - Ranking dos 10 Países com maior % de Retalho Online no Total de Vendas de Retalho entre 2021 & 2022

Top 10 Countries, Ranked by Retail Ecommerce Sales Share, 2021 & 2022

% of total retail sales

	2021	2022
1. China	52.1%	55.6%
2. South Korea	28.9%	31.6%
3. UK	28.3%	28.5%
4. Denmark	19.1%	19.8%
5. Norway	17.6%	17.7%
6. US	15.0%	16.3%
7. Finland	14.3%	14.4%
8. Sweden	13.2%	13.8%
9. France	11.2%	11.7%
10. Spain	10.9%	11.2%

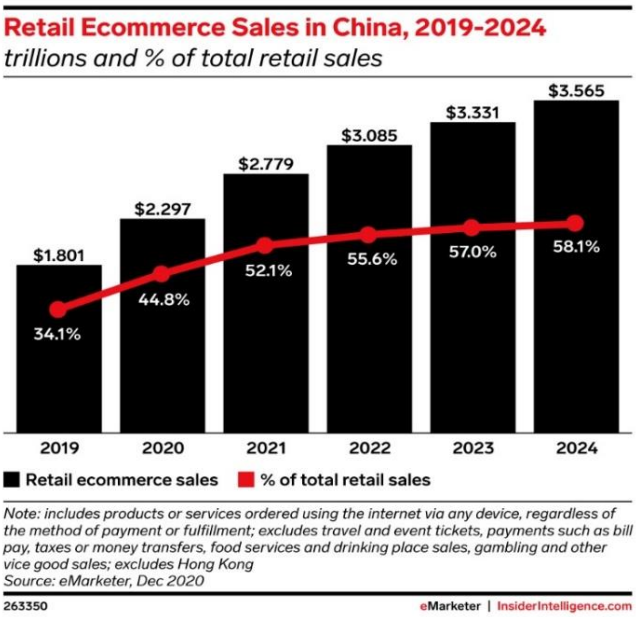
Note: includes products or services ordered using the internet via any device, regardless of the method of payment or fulfillment; excludes travel and event tickets, payments such as bill pay, taxes or money transfers, food services and drinking place sales, gambling and other vice good sales
Source: eMarketer, Dec 2020

263351 eMarketer | InsiderIntelligence.com

Fonte: (eMarketer, 2020)

Por outro lado, é de salientar também o bom desempenho da economia e do retalho chinês, dada a sua competitividade tecnológica e o investimento em infraestrutura [16] . No setor do retalho chinês, o retalho online tem vindo a crescer significativamente nos últimos anos, sendo que, em 2021, é expectável que mais de 50% do total das vendas de retalho pertença ao *e-commerce* [17] .Na Figura 4, podemos ver como o *e-commerce* chinês se foi desenvolvendo e como é esperado que se desenvolverá até 2024.

Figura 3 - Vendas de Retalho Online na China entre 2019 & 2024



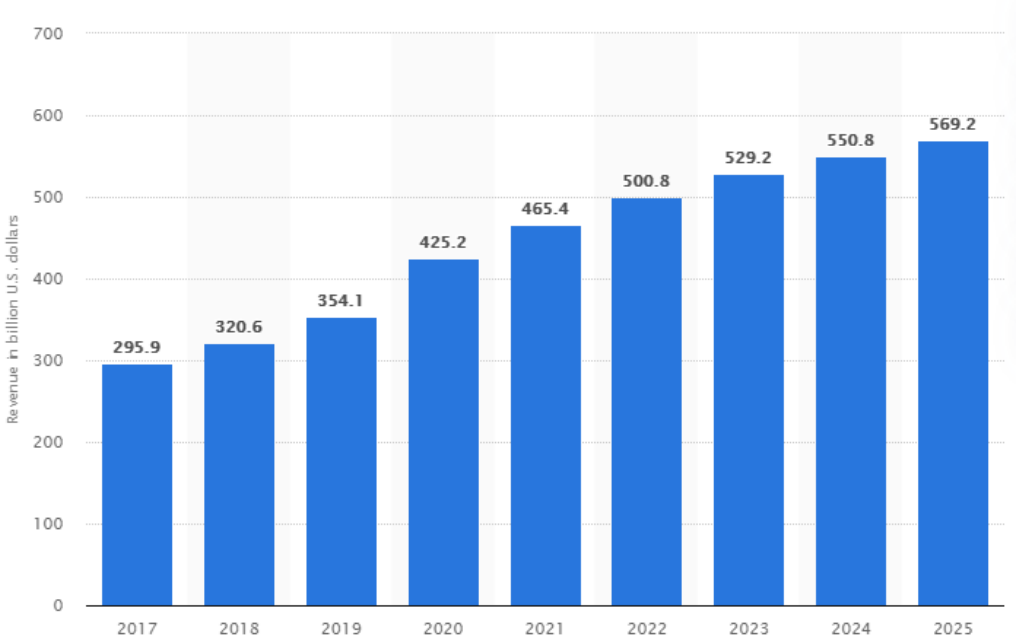
Fonte: (eMarketer, 2020)

[16] (Deloitte, 2021)
[17] (Cramer-Flood, 2021)

Na Zona Euro, em março de 2021, o volume de comércio de retalho aumentou 12%, em termos homólogos, e cerca de 2,7% comparativamente com fevereiro de 2021. Na UE, o volume de vendas deste setor também aumentou 11,6%, em termos homólogos, e em 2,6% relativamente ao mês anterior [18].

Entre 2014 e 2019, o retalho online na Europa aumentou de 7% para 12%, no entanto, os impactos gerados pela pandemia e pelas consequentes medidas levaram à utilização do comércio eletrônico enquanto método mais seguro para comprar bens não-essenciais. Nesse sentido, as vendas no retalho online aumentaram cerca de 31% face aos últimos anos e, dessa forma, aumentando também a sua quota parte das vendas de retalho para cerca de 16% [19]. Tendo isto em conta, é expectável que os rendimentos do retalho online continuem a aumentar na Europa, tal como podemos ver na Figura 5.

Figura 4 - Previsão das receitas do Retalho Online na Europa entre 2017 e 2025



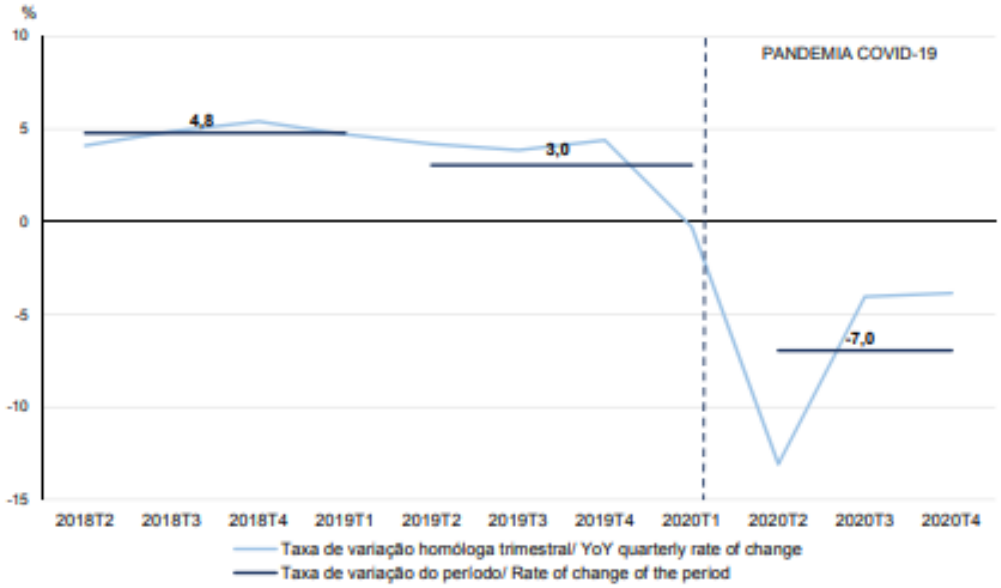
Fonte: (Rotar, 2021)

2.1.2 - Caracterização Atual do Setor do Retalho a nível nacional

Em 2021, o valor do PIB português, em termos nominais, diminuiu cerca de 7% entre o 2º e o 4º Trimestre de 2020, sendo que a variação mais negativa (-13,2%) se deu no 2º Trimestre de 2020, ou seja, aquando da implementação das medidas mais restritivas no combate ao COVID-19 (ver figura 6).

[18] (Eurostat, 2021)
[19] (Savills, 2020)

Figura 5 - Variações do PIB de Portugal no antes e durante a pandemia



Fonte: (Instituto Nacional de Estatística, 2021)

Dados estes constrangimentos, o setor do Comércio a Retalho em Portugal, tal como em outros Estados, foi severamente impactado tendo registado uma quebra de 1,5%, face a 2019, no volume de vendas. No entanto, nem todas as indústrias deste setor foram afetadas da mesma forma [20].

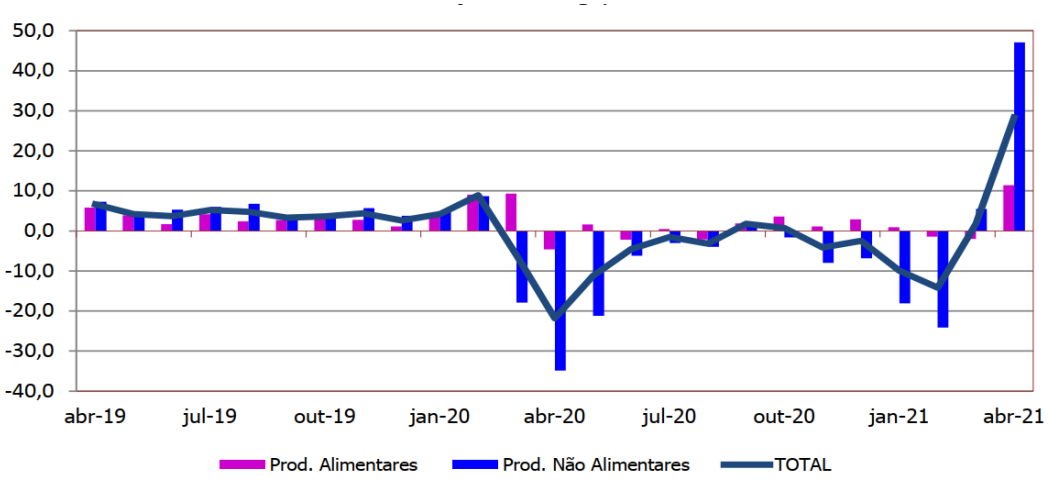
O retalho alimentar registou um significativo aumento de vendas de 8,1% em 2020 comparativamente com 2019. Contudo, o retalho não-alimentar ou especializado registou uma quebra de cerca de 18% relativamente ao ano anterior e uma quebra de cerca de 74% relativamente ao VAB. Dentro deste, a indústria do vestuário foi a mais afetada, com 60% das empresas a registaram quebras superiores a 50%. Em contrapartida, os serviços de telecomunicações registaram um aumento da atividade e uma melhor adaptação às medidas de confinamento[21] . O recurso ao comércio eletrônico, segundo o INE, contribuiu para que esta redução não tivesse sido mais significativa [22].

O efeito da crise pandémica acelerou o crescimento do retalho *online* em Portugal, representando este, em 2020, 8,6% do total de compras realizadas pelos consumidores[23] . Além disso, os novos padrões de consumo levaram a que 47% dos portugueses tenham comprado pelo menos um produto via *online* [24].

Apesar dos impactos negativos sentidos pelo setor em 2020, o ano de 2021 já mostra uma nota positiva, sendo que o volume de negócios no comércio a retalho apresentou em abril do presente ano, segundo o INE, um aumento de 28,3% face a abril do ano anterior, com um crescimento significativo do setor do Retalho Não Alimentar [25].

[20] (Associação Portuguesa de Empresas de Distribuição, 2021)
[21] (Pais Mamede, Pereira, & Simões, 2020)
[22] (Instituto Nacional de Estatística, 2021)
[23] (Associação Nacional dos Industriais de Laticínios, 2020)
[24] (ecommerceDB, 2019)
[25] (Instituto Nacional de Estatística, 2021)

Figura 6 - Variações Homólogas no Volume de Negócios do Comércio a Retalho



Fonte: (Instituto Nacional de Estatística, 2021)

2.1.3 - Do Canal Único para o Retalho Multicanal até ao Retalho Omnicanal

Os canais são vistos como pontos intermédios que facilitam a interação e as trocas comerciais entre o consumidor e o fornecedor. Nesse sentido, um "*canal*" pode ser definido como um "*ponto de contacto ou um meio pelo qual a empresa e o consumidor interagem*" [26]. Estudos afirmam que existem 3 canais pelos quais os consumidores conseguem fazer as suas compras: o tradicional ou físico, *web* e *mobile* [27].

Antes do avanço do retalho para a dimensão digital, as empresas utilizavam apenas um tipo de canal para comunicar com os seus clientes. Estes canais podiam adquirir a forma de loja física, de um catálogo ou até mesmo de vendas à distância [28]. Os avanços tecnológicos das últimas décadas permitiram a proliferação de possíveis canais pelos quais as empresas podem interagir com os consumidores. Dessa forma, as vendas à distância começaram a integrar o conteúdo do canal digital [29].

A utilização simultânea de vários canais, por sua vez, levou à ideia do retalho multicanal, ou seja, "*o conjunto de atividades envolvidas na venda de produtos ou serviços aos consumidores através de mais do que um canal*" [30]. Neste contexto, enquanto os consumidores interagem com a empresa através de vários canais, o foco da empresa vira-se para a gestão e otimização de cada canal separadamente.

Embora a utilização de vários canais seja a norma, a interação dos consumidores através de múltiplos canais levantou a necessidade de atingir a integração dos canais para permitir que os consumidores possam ter uma experiência de compra sem restrições. Uma resposta a esta questão surgiu sob a forma de Canais Cruzados ou *Cross-Channel* que se baseia na integração

[26] (Neslin, et al., 2006)
[27] (Dennis, Alamanos, Papagiannidis, & and Bourkakis, 2014)
[28] (Decreto-Lei 24/2014)
[29] (Dennis, Alamanos, Papagiannidis, & and Bourkakis, 2014)
[30] (Zhang, et al., 2010)

parcial de vários canais, permitindo ao consumidor mudar entre certos canais, mas não entre todos [31].

Uma característica essencial deste modelo de gestão de canais é que não se limita a canais, mas também integra pontos de contacto ou *touchpoints,* isto é, "*um episódio de contacto direto ou indireto com uma marca ou empresa*" [32], como por exemplo, anúncios, redes sociais, TV, entre outros. Apesar de oferecer um certo patamar de integração e interação através dos canais e pontos de interação, a falta de integração completa significa que cada canal tem os seus objetivos e a sua própria gestão e os dados não podem ser partilhados por todos os canais e pontos de interação.

Nesse sentido, de forma a dar resposta à questão à integração completa necessária, surgiu o modelo de gestão omnicanal. Este entende-se como um "*conjunto de atividades ligadas à venda de mercadorias ou serviços através de todos os canais disponíveis*", podendo integrar as suas lojas físicas no seu website ou em formato *mobile* [33]. Chopra descreve o omnicanal como a *"utilização de uma variedade de canais para interagir com os consumidores e satisfazer os seus pedidos*" [34] enquanto que Vorhoef vai mais longe ao descrever o omnicanal como a "*gestão sinergética dos vários canais disponíveis e dos pontos de contato com o cliente, de forma que o cliente a experiência nos canais e o desempenho nos canais são otimizados*"[35].

Deste ponto, podemos concluir que o omnicanal é visto como uma estratégia de otimização dos vários canais de uma forma colaborativa e unificada, ao contrário da abordagem multicanal que vê os canais como meios totalmente independentes uns dos outros e da abordagem *Cross-Channel,* que apenas permite a integração de alguns canais. De forma mais simplificada, na figura 1, podemos ver as características de cada um dos modelos de gestão de canais.

Tabela 1 - Diferenciação dos Conceitos de Gestão de Canais

Característica	**Multi-Canal**	**Canal-Cruzado**	**Omnicanal**
Entrega de Informação	Canais	Canais & Touchpoints	Canais & Touchpoints
Integração	Trocar entre canais não é possível	Troca entre certos canais e touchpoints é possível	Troca entre canais e touchpoints é possível sem barreiras
Gestão	Separado por canal	Por canal ou canais e touchpoints conectados	Através de todos os canais e touchpoints
Objetivos	Definidos por canal	Por canal ou canais e touchpoints conectados	Através de todos os canais e touchpoints
Interação	Interacção bilateral	Interação bilateral ou multilateral	Interação bilateral ou multilateral
Dados	Dados não são partilhados entre canais	Dados são parcialmente partilhados entre canais	Dados são partilhados através de todos os canais

Fonte: (Mirsch, Lehrer, & Jung, 2016)

[31] (Mirsch, Lehrer, & Jung, 2016)
[32] (Verhoef, Kannan, & Jeffrey, From Multi-Channel Retailing to Omni-Channel Retailing, 2015)
[33] (Beck & Rygl, 2015)
[34] (Chopra, 2018)
[35] (Verhoef, Kannan, & Jeffrey, From Multi-Channel Retailing to Omni-Channel Retailing, 2015)

2.1.4 - As particularidades do Retalho Omnicanal

Tal como verificamos anteriormente, estas constantes mudanças dos padrões de consumo e a emergência de novas tecnologias levaram à necessidade de implementar uma estratégia que consiga gerir as múltiplas interações entre marca e consumidor. Com isto, surge o modelo omnicanal como resposta às necessidades dos consumidores e às operações menos eficientes dentro da cadeia de abastecimento. Enquanto modelo de gestão, o omnicanal apresenta algumas particularidades únicas que mais nenhum modelo oferece por completo. Existem 3 pontos dentro das organizações onde o retalho omnicanal atua principalmente, sendo estas a experiência do consumidor, o marketing e a Cadeia de Abastecimento [36].

Neste subcapítulo, iremos abordar como o retalho omnicanal se diferencia nestas 3 áreas de atuação.

2.1.4.1 - Experiência do consumidor

Na década de 50, a noção de que as pessoas procuram experiências satisfatórias e não apenas produtos começou a ser estudada de uma forma mais detalhada [37]. Esta perspetiva continuou a ser explorada mais tarde, sobretudo quando estudos comprovaram o papel dos aspetos mais emotivos na tomada de decisões e na experiência [38]. Ou seja, esse ponto de vista leva à ideia de que uma experiência passa pela sua compra para que "*o consumidor possa passar tempo a desfrutar de uma série de eventos memoráveis que uma empresa prepara*"[39].

De outra perspetiva, estudos debatem que existe uma visão mais ampla para a experiência do consumidor, ao argumentar que *"todo o serviço leva a uma experiência do consumidor, independentemente da sua natureza ou forma"* [40]. Esta visão expansiva da experiência do consumidor abre espaço para um entendimento multidimensional que engloba as respostas cognitivas, afetivas, emocionais, sociais e físicas dos consumidores. Assim como também engloba toda experiência do consumidor *"incluindo a pesquisa, a fase de compra, consumo e pós-venda da experiência, e pode envolver múltiplos canais de venda a retalho"*. Desta forma, a experiência do consumidor é holística na sua essência [41].

A chegada e o desenvolvimento de novas tecnologias trouxeram consigo grandes mudanças na experiência de compra do consumidor. Uma destas alterações passa pela capacidade dos consumidores interagirem com a marca através de múltiplos *touchpoints* tanto na esfera *online* como *offline*. Como resposta, os retalhistas procuram uma solução que crie experiências mais holísticas [42].

Isto é verificável através do comportamento de algumas marcas que começaram como retalhistas exclusivamente digitais, mas que optaram por abrir lojas físicas ao longo dos últimos anos. Por exemplo, a Amazon, uma das maiores empresas de e-Commerce do mundo [43], ao longo dos últimos anos tem vindo a mudar para o mundo offline porque já percebeu as

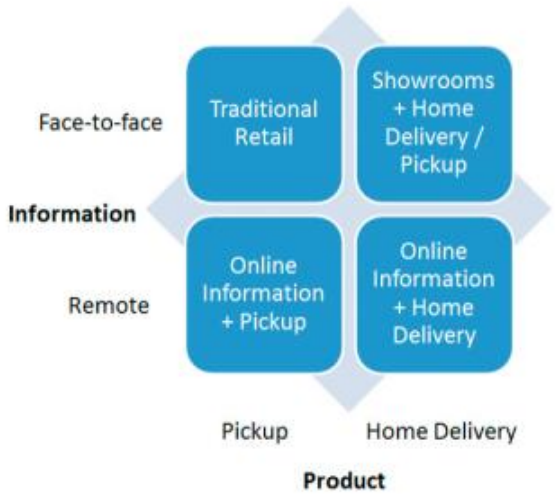
[36] (Jocevskim, Arvidsson, Miragliotta, Ghezzi, & Mangiaracina, 2019)
[37] (Abbott, 1955)
[38] (Holbrook & Hirschman, 1982)
[39] (Pine & Gilmore, 1998)
[40] (Brakus, Schmitt, & Zarantonello, 2009)
[41] (Verhoef, et al., 2009)
[42] (Kahn, Inman, & Verhoef, 2018)
[43] (Pajovic, 2020)

vantagens que uma loja física lhe pode proporcionar [44]. Outro exemplo, é caso do eBay que também se está a mudar para um modelo omnicanal de forma a adaptar-se aos novos padrões de consumo [45].

Tendo isto em conta, a transformação da experiência do consumidor tornou-se um aspecto-chave do retalho omnicanal. Através de uma integração dos canais de venda, é alterado o paradigma do retalho, concentrando-se assim na criação de uma experiência de compra sem barreiras e única, em detrimento do foco na transação. Esta interação entre os canais de venda e os consumidores assenta no balanço de 3 tipos de fluxos – informação, de produto e de fundos. O retalhista comunica o preço e o produto, e, por sua vez, o consumidor faz uma encomenda e realiza o pagamento. A informação da encomenda é então utilizada pelo retalhista para fazer chegar o produto ao consumidor [46].

Considerando a interação entre marca e consumidor neste formato, dentro da estratégia omnicanal existem 4 modelos para a troca de informações e de produtos, como podemos ver na figura 8.

Figura 7 - Modelos de Fluxos de Informação e Produto dentro da Estratégia Omnicanal



Fonte: (Chopra, 2018)

O Retalho Tradicional tem por base a loja física como único canal de vendas, onde o fluxo de informações e do produto é feito presencialmente e através de uma interação cara-a-cara. Por outro lado, temos o modelo puramente digital ou *e-tailers*, que utiliza o *online* enquanto o único canal de vendas, seja pela *web* ou em formato *mobile*. Neste modelo, o fluxo de informações e de produtos é feito através da *internet* com entrega diretamente em casa. O aparecimento da estratégia de múltiplos canais traz 2 novos modelos inovadores para o fluxo de informações e produtos entre entidade e consumidor. Em primeiro lugar, o conceito de *showrooming*, onde o consumidor se desloca até à loja física de forma a adquirir mais informação, com a possibilidade de posteriormente encontrar preços mais competitivos independentemente do canal escolhido e entrega à escolha do consumidor. Em segundo lugar, o conceito de

[44] (Schaverien, 2018)
[45] (WARC, 2013)
[46] (Chopra, 2018)

webrooming, onde o consumidor recolhe informações via *online* e efetua a compra numa loja física. Através deste modelo, os retalhistas conseguem gerar maior tráfego das suas plataformas digitais e garantir as vendas nas lojas físicas. Como podemos verificar através destes modelos, a integração dos canais de vendas é um elemento-chave para a interação com o consumidor e para lhe fornecer uma experiência de compra consistente. Dessa forma, as empresas têm procurado desenvolver os seus conceitos de negócio para ir ao encontro das novas necessidades de cada consumidor[47].

2.1.4.2 - Sistemas de análise

Tal como se verifica anteriormente, a integração dos canais de venda oferece várias vantagens aos consumidores no que diz respeito à sua experiência de compra e à sua interação com a empresa. No entanto, este processo implica a utilização e análise de dados reunidos num canal de forma a serem aproveitados noutro [48].

Neslin & Shankar refletem e sublinham a necessidade da integração dos canais de venda de forma a obter uma visão comum sobre o cliente e gerir melhor os clientes[49]. Além disso, Arora & Sahney defendem a utilização dos dados adquiridos num canal de forma a melhorar experiências noutros canais de forma a criar vantagens para a empresa[50].

A análise de dados integrada é a espinha dorsal de todas as atividades "*front-end"* do retalho [51]. Isto permite uma interação com o consumidor ao longo dos diferentes canais com uma perspetiva global. Por exemplo, aquando a compra de um produto numa loja física, o consumidor deverá abrir uma nova conta de cliente. Contudo, aquando a compra de um produto na loja *online* do mesmo retalhista, deverá novamente abrir uma nova conta.

2.1.4.3 - Logística e Cadeias de Abastecimento

De forma a que a experiência do consumidor seja melhor, é importante considerar o papel das cadeias de abastecimento dentro do retalho omnicanal. Estudos afirmam que a *"gestão da cadeia de abastecimento deve ser coordenada e integrada através dos vários canais"* Contudo, a transição para uma estratégia omnicanal requer a restruturação da cadeia de abastecimento de forma a atingir a flexibilidade organizacional pretendida[52].

Por exemplo, tendo em conta que a personalização é um dos aspetos-chave do retalho omnicanal, os produtores deixam de produzir em grandes quantidades para se focarem na produção de séries mais reduzidas e personalizadas, o que, por sua vez, agiliza as suas cadeias de abastecimento. A aproximação entre o *online* e *offline,* que o retalho omnicanal confere, leva a uma maior preponderância da loja física dentro da cadeia de abastecimento. A partir destas, é possível tornar os processos (recolhas, entregas e devoluções de artigos, gestão de *stocks,* ...) mais ágeis e com um custo mais baixo[53].

[47] (Chopra, 2018)
[48] (Jocevskim, Arvidsson, Miragliotta, Ghezzi, & Mangiaracina, 2019)
[49] (Neslin & Shankar, 2009)
[50] (Arora & Sahney, 2017)
[51] (Jocevskim, Arvidsson, Miragliotta, Ghezzi, & Mangiaracina, 2019)
[52] (Jocevskim, Arvidsson, Miragliotta, Ghezzi, & Mangiaracina, 2019)
[53] (Cunha, 2015)

Por exemplo, a uma das razões pelas quais a Amazon está a mover-se para o omnicanal é a pressão que os custos de envio têm nas cadeias de abastecimento. Dessa forma, ao ter acesso a um espaço físico, a empresa consegue reduzir os custos de envio, enquanto pode atrair consumidores que estão a levantar a sua encomenda e impulsioná-los a comprar mais dentro da loja [54].

À semelhança da Amazon, alguns retalhistas já começaram a utilizar as lojas físicas, em detrimento dos centros de distribuição, de forma a garantirem entregas rápidas e a cobrirem áreas geográficas mais distantes [55]. Outros formatos encontrados pelos retalhistas de forma a irem ao encontro das necessidades dos seus consumidores incluem a criação de pontos de conveniência ou até mesmo *lockers* em estações de metro, comboio ou aeroportos [56].

2.1.5 – Personalização

A ideia de personalização de fornecer ao consumidor o produto ou serviço certo, no momento certo e no local certo é algo que tem vindo a ser debatido e nenhuma definição é universalmente aceite [57]. Alguns defendem que se trata individualização, outros argumentam a favor da segmentação, no entanto, numa versão mais comummente referida, estipula-se que a personalização se trata de qualquer estratégia de marketing individualizada e direcionada [58]. Nesse sentido podemos considerar a personalização como "uma adaptação do produto e da experiência de compra às suas vontades, necessidades e preferências do consumidor, consoante a sua informação pessoal e de preferências" [59].

Nas lojas físicas, isto significa servir os clientes de forma individualizada para satisfazer suas necessidades [60], enquanto no mundo digital, os retalhistas podem rastrear os hábitos de compra anteriores dos clientes com tecnologias de personalização [61]. Retalhistas omnicanal, dada a sua natureza centrada no cliente, retira benefícios da personalização pois, além de produtos, serviços e até mesmo interações personalizadas que apelam aos consumidores [62], esta também permite uma maior flexibilização nas transações e anúncios mais direcionados [63].

Em termos legais, tendo em conta esta perspetiva, a personalização pode ser definida como "*a coisa que não sendo pré-fabricada, é produzida com base numa escolha individual ou numa decisão do consumidor*", ou por outras palavras, bem produzido segundo as especificações do consumidor [64].

[54] (Schaverien, 2018)
[55] (Chaturvedi, Martich, Ruwadi, & Ulker, 2013)
[56] (Cunha, 2015)
[57] (Riegger, Klein, Merfeld, & Henkel, 2020)
[58] (Sunikka & Bragge, 2012)
[59] (Chellappa & Sin, 2005)
[60] (Shen & Ball, 2009)
[61] (Zhang, Agarwal, & Lucas, 2011)
[62] (Ansari & Mela, 2003)
[63] (Kalaignanam, Kushwaha, & Rajavi, 2018)
[64] (Ministério Público, 2014)

2.2 - Privacidade - Conceitos Base e Jurídicos

Privacidade pode ser definida como um direito moral das pessoas singulares ou coletivas a serem livres de vigilância ou interferência por parte de outros indivíduos ou organizações [65], protegendo assim a sua intimidade [66].

Apesar das suas manifestações iniciais em documentos históricos como a Magna Carta Inglesa de 1215, a Constituição Francesa de 1791 e a Constituição dos EUA, o direito à privacidade foi apenas exposto e desenvolvido, pela primeira vez, em 1890 com a publicação do artigo *"Right to Privacy"* na Harvard Law Review de Samuel Warren e Louis Brandeis. Posteriormente, múltiplas entidades estatais e interestatais foram adotando este princípio, como a Declaração Universal dos Direitos do Homem e Declaração Americana de Direitos e Deveres do Homem, ambas de 1948, a Convenção Europeia dos Direitos do Homem de 1950 e o Pacto Internacional relativo aos deveres cívicos e políticos de 1966 [67] .

Em termos jurídicos portugueses, a Privacidade ou o direito à reserva sobre a intimidade da vida privada é abordado na CRP, ao anunciar 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 proteção legal contra quaisquer formas de discriminação"* [68].

2.2.1 - Proteção de Dados Pessoais / Privacidade da Informação Pessoal

A Privacidade da Informação ou Proteção de Dados Pessoais é um ramo da privacidade. Este termo entende-se então pela necessidade de controlo, por parte de uma pessoa singular ou coletiva, sobre que e como é utilizada a informação que lhe diz respeito. A aprovação da primeira lei de proteção de dados pessoais remonta até 1970, em Hessen, na Alemanha. Em 1973, a Suécia aprovou uma lei a nível nacional nesta matéria. Mais tarde, o direito à proteção de dados foi sendo incorporado por acordos supranacionais e organizações internacionais como a OCDE, o Conselho da Europa e UE [69].

Em Portugal, o direito à proteção de dados pessoais foi consagrado na CRP de 1976, a primeira constituição do mundo a proteger expressamente este direito [70]. De acordo com o documento, este reconhecia a todos os portugueses o direito à *"intimidade da vida privada e familiar"*, assim como, também permitia aos cidadãos ter *"conhecimento do que constar de registos mecanográficos a seu respeito, retificar e atualizar esses mesmos dados, impedindo o tratamento de dados referentes a convicções políticas, religiosas ou de vida privada"* [71]. Paralelamente, o Código Civil português também estipula este direito ao reafirmar que *"todos devem guardar reserva quanto à intimidade da vida privada de outrem"* [72].

[65] (Laudon & Traver, 2017)
[66] (Lobato & Zorzo)
[67] (Correia & Jesus, 2014)
[68] Art. 26º da CRP
[69] Art. 33º da CRP/1976
[70] (Correia & Jesus, 2014)
[71] Art. 35º da CRP/1976
[72] Art. 80º do Código Civil Português

Ao longo dos anos, com as revisões constitucionais às quais a CRP esteve sujeita, foram-se estabelecendo melhores salvaguardas para a proteção de dados dos cidadãos portugueses. Desde a proibição ao acesso de terceiros e interconexão de ficheiros com dados pessoais até à criação de uma entidade independente que garanta a proteção dos dados, a CRP e Portugal foram-se sempre mantendo na liderança nesta matéria.

Capítulo III – O RGPD: Considerações Iniciais

3.1 – Definições

3.1.1- Dados Pessoais

O termo "Dados Pessoais" pode ser definido como uma informação ou informações de qualquer natureza, em qualquer formato, que permitam identificar, direta ou indiretamente, a pessoa singular através de um identificador como o nome ou número de identificação, ou através de características do foro físico, fisiológico, mental, socioeconômico ou cultural. A recente legislação salvaguarda também um estatuto especial para "*dados pessoais sensíveis*", incluindo dados de saúde, biométricos, genéticos, da vida sexual, filiação sindical, origem étnica ou racial, assim como opiniões e convicções políticas e religiosas[73].

3.1.2 - Ficheiro

O conceito Ficheiro é definido como "qualquer conjunto estruturado de dados pessoais, acessível segundo critérios específicos, quer seja centralizado, descentralizado ou repartido de modo funcional ou geográfico"[74].

3.1.3 - Tratamento de Dados Pessoais

O tratamento dos dados pessoais é o núcleo da aplicação do RGPD, dado que é este que espoleta verdadeiramente a aplicação da Proteção de Dados [75]. O conceito de tratamento é definido como uma operação ou operações, automatizados ou não, realizadas sobre dados pessoais. Tais operações podem incluir *"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 [...] disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição"*[76].

Desta forma, o conceito de tratamento consiste em 3 elementos-base: a) uma operação ou operações, isto é, um acontecimento real, produzido por uma manifestação humana que produz efeitos jurídicos; b) realizadas sobre dados pessoais, ou seja, qualquer dado que não seja relativo a pessoas singulares ou que não seja reconduzível ao conceito de dado pessoal; c) por meios automatizados ou por meios não automatizados, sendo que o RGPD se aplica *"ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos em ficheiros ou a eles destinados"*[77] [78].

[73] Art. 4º nº1 do RGPD
[74] Art. 4º nº6 do RGPD
[75] (Barreto, 2020)
[76] Art. 4º nº2 do RGPD
[77] Art. 2º nº1 do RGPD
[78] (Barreto, 2020)

3.1.4 - Limitação do Tratamento

Implantação de um limite nos dados pessoais preservados de forma a reduzir o seu tratamento no futuro[79].

3.1.5 - Responsável pelo Tratamento

Entidade que, individualmente ou em conjunto com outras, define os objetivos e métodos de tratamento de dados pessoais [80].

3.1.6 - Violação de Dados Pessoais

Quebra de segurança, acidental ou não, que implique "a perda, alteração, divulgação ou acesso, não autorizados, a dados pessoais conservados ou sujeitos a qualquer outro tipo de tratamento" [81].

3.1.7 – *Profiling* ou Definição de Perfis

Qualquer tipo de tratamento automatizado de dados pessoais que tenha como objetivo a avaliação de determinadas características pessoais de uma pessoa singular, como *"o seu desempenho profissional, a sua situação económica, situação de saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações"* [82].

3.1.8 - Pseudonimização

Tratamento de dados pessoais que possibilitem a anonimização de um titular de dados, sem recorrer a informações adicionais e desde que essas mesmas informações adicionais sejam preservadas separadamente e sejam sujeitas a medidas que também possibilitem a anonimização do titular de dados[83].

3.1.9 - Subcontratante

Pessoa singular ou Entidade que trate os dados pessoais sob a responsabilidade do responsável pelo seu tratamento[84].

3.1.10 - Destinatário

Pessoa Singular ou Entidade que recebe comunicações de dados pessoais, sendo ou não um terceiro. Embora as autoridades públicas possam receber dados pessoais no âmbito de inquéritos, estas não são consideradas destinatários[85].

[79] Art. 4º nº3 do RGPD
[80] Art. 4º nº7 do RGPD
[81] Art. 4º nº12 do RGPD
[82] Art. 4º nº4 do RGPD
[83] Art. 4º nº5 do RGPD
[84] Art. 4º nº8 do RGPD
[85] Art. 4º nº9 do RGPD

3.1.11- Terceiro

Pessoa Singular ou Entidade autorizada a tratar os dados pessoais mesmo "que, não sendo o titular dos dados, o responsável pelo tratamento, o subcontratante e as pessoas que, sob a autoridade direta do responsável pelo tratamento ou dos subcontratantes" [86].

3.1.12 - Estabelecimento Principal

Referente a um subcontratante com estabelecimentos em mais do que um Estado-Membro, o local onde se encontra a sua administração central dentro da União ou, se não existir uma na União, o estabelecimento dentro da União onde são desempenhadas as principais atividades de tratamento no contexto das atividades de um estabelecimento do subcontratante[87].

3.1.13 - Regras Vinculativas Aplicáveis às Empresas

De acordo com o art.º 4, nº 20 do RGPD, as Regras Vinculativas Aplicáveis às Empresas são definidas como "as regras internas de proteção de dados pessoais aplicadas por um responsável pelo tratamento ou um subcontratante estabelecido no território de um Estado-Membro para as transferências ou conjuntos de transferências de dados pessoais para um responsável ou subcontratante num ou mais países terceiros, dentro de um grupo empresarial ou de um grupo de empresas envolvidas numa atividade económica conjunta" [88].

3.1.14 - Autoridades de Controlo

Nos termos do art.º 4º, nº 21 do RGPD, uma autoridade de controlo é definida como *"uma autoridade pública independente criada por um Estado-Membro"*. Outras autoridades de controlo, salvaguardadas pelo regulamento, incluem as Autoridades de Controlo Interessadas, isto é, *"afetadas pelo tratamento de dados pessoais seja porque o responsável pelo tratamento ou o subcontratante está estabelecido no território do Estado-Membro dessa autoridade de controlo, os titulares de dados que residem no Estado-Membro dessa autoridade de controlo são substancialmente afetados, ou suscetíveis de o ser, pelo tratamento dos dados ou ter sido apresentada uma reclamação junto dessa autoridade de controlo"* [89].

3.2 - Análise do Regulamento

3.2.1 - Princípios Subjacentes

3.2.1.1 - Princípio da Licitude, Lealdade e Transparência

O princípio da Licitude, Lealdade e Transparência, conforme refere o art.º 5, nº 1, al. a) do RGPD, explica que os dados pessoais são *"objeto de um tratamento lícito, leal e transparente em relação aos titulares de dados"* [90].

Este princípio pode ser dividido em 3 princípios distintos. O tratamento lícito dos dados pessoais implica que deverão *"ser tratados com base no consentimento da titular dos dados em causa ou noutro fundamento legítimo"*, assim como pressupõe o cumprimento do RGPD e

[86] Art. 4º nº10 do RGPD
[87] Art. 4º nº16 do RGPD
[88] Art. 4º nº20 do RGPD
[89] Art. 4º nº 21 & 22 do RGPD
[90] Art. nº5 nº1 do RGPD

das leis aplicáveis. Este conceito de consentimento, um dos princípios mais importantes do RGPD, será abordado posteriormente neste capítulo.

O princípio da lealdade estipula que os dados pessoais serão utilizados em conformidade com a finalidade a que se destinam, consolidando a relação entre a organização e o titular dos dados. Dessa forma, este princípio funciona como um reforço do princípio de licitude e *"permite contestar determinados comportamentos que dificilmente poderiam ser descritos como violadores"* [91].

O princípio da Transparência impõe que as informações relacionadas com os dados pessoais ou o seu tratamento seja de acessível e compreensível facilmente, assim como, a linguagem e os procedimentos de transmissão da informação utilizados deverão ser claros, concisos e simples. Consequentemente, o princípio da transparência é transversal a todo o processo de recolha e tratamento de dados[92]

3.2.1.2 - Princípio da Limitação de Finalidades

De acordo com o art.º 5, nº1, al. b) do RGPD, o princípio da Limitação de Finalidades pode ser descrito como a recolha de dados pessoais "*... para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades"*[93].

Este princípio assenta na ideia de que as finalidades deverão ser a) determinadas, ou seja, são determinadas antes do início do processo iniciar, devendo para isso ser realizado um exame prévio para o levantamento e fundamentação dos propósitos e não podendo ser utilizados para um fim distinto daquele para qual foi incialmente recolhido.; b) explícitas, isto é, as finalidades, na forma como são expostas a todas as entidades, deverão ser o mais claras possíveis; e c) legítimas ou que não violem as leis aplicáveis[94].

3.2.1.3 - Princípio da Minimização de Dados

Conforme o art.º 5, nº 1, al. c) do RGPD, o princípio da Minimização de Dados é definido como os dados pessoais que são *"adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados"*[95].

Este princípio pressupõe 3 componentes principais: a) adequação, ou seja, os dados pessoais devem enquadrar-se nas finalidades determinadas; b) pertinência, isto é, os dados pessoais devem contribuir positivamente para a prossecução das finalidades; c) necessidade, tendo vista que apenas são tratados os dados pessoais necessários às finalidades estipuladas.

Este princípio estipula então que os dados, ao serem recolhidos, deverão ser limitados aos fins que se destinam, não podendo ser utilizados para outra finalidade não consentida pelo titular, atuando assim como um reforço da limitação de finalidades. Dessa forma, o tratamento dos dados para outros fins necessitará do consentimento do seu titular [96].

---

[91] (Barreto, 2020)
[92] (Barreto, 2020)
[93] Art. nº5 nº1 do RGPD
[94] (Barreto, 2020)
[95] Art. nº5 nº1 do RGPD
[96] (Barreto, 2020)

3.2.1.4 - Princípio da Exatidão

Tal como descrito no art.º 5, nº 1, al. d), o princípio da Exatidão prevê os dados pessoais como "exatos e atualizados sempre que necessário; devem ser adotadas todas as medidas adequadas para que os dados inexatos, tendo em conta as finalidades para que são tratados, sejam apagados ou retificados sem demora" [97].

A partir desta definição pode-se destacar: a) a proibição de recolher ou armazenar dados incorretos; b) o dever de atualização dos dados, sempre que necessário; e c) o dever de retificar ou apagar dados incorretos, consoante as finalidades. Nesse sentido, este princípio exige que o responsável pelo tratamento dos dados disponha das ferramentas necessárias para a atualização, retificação ou potencial eliminação dos dados [98].

3.2.1.5 - Princípio da Limitação de Conservação

O princípio da Limitação de Conservação é descreve, no art.º 5, nº 1, al. e), que os dados pessoais são "conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados"[99]

Este princípio, tal como está descrito acima, delimita a nível temporal a utilização dos dados pessoais recolhidos, podendo apenas mantê-los por um certo período de tempo, salvaguardando exceções que sejam do interesse público (investigação científica, fins estatístico,…). Nesse sentido, o responsável pelo tratamento estipula os prazos para o apagamento ou revisão periódica consoante a sua necessidade[100].

3.2.1.6 - Princípio da Integridade e Confidencialidade

O princípio da Integridade e Confidencialidade, de acordo com o art.º 5, nº 1, al. f) do RGPD, estipula que os dados pessoais são *"tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando as medidas técnicas ou organizativas adequadas"*[101].

Segundo este princípio, as entidades deverão adotar medidas de segurança contra potenciais violações e invasões, tanto físicas como digitais. Este conceito de segurança abrange a destruição, perda ou danificação dos respetivos dados, independentemente do impacto [102].

3.2.1.7 - Princípio da Responsabilidade

O princípio da responsabilidade, descrito no art.º 5 nº 2 do RGPD, pressupõe que o responsável pelo tratamento de dados *"é responsável pelo cumprimento do disposto no n.º 1 e tem de poder comprová-lo"*[103]. Ou seja, o responsável pelo tratamento de dados deve garantir e certificar-se do cumprimento de todos os princípios enunciados anteriormente, assim como deve conseguir demonstrar esse cumprimento às autoridades de controlo e aos tribunais aquando necessário.

[97] Art. nº5 nº1 do RGPD
[98] (Barreto, 2020)
[99] Art. nº5 nº1 do RGPD
[100] (Barreto, 2020)
[101] Art. nº5 nº1 do RGPD
[102] (Barreto, 2020)
[103] Art. nº5 nº1 do RGPD

Não obstante, este dever aplica-se tanto ao responsável pelo tratamento, ao subcontratante e ao terceiro, aquando autorização para tratar os dados pessoais [104].

3.2.1.8 - Princípio do Consentimento

Tal como disposto no RGPD, o conceito de consentimento pode ser definido como "uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento" [105].

O consentimento manifesta-se neste regulamento como o principal alicerce da legitimidade para o tratamento dos dados pessoais e o seu princípio, resultado do art.º 7 do RGPD, declara que o responsável pelo tratamento dos dados pessoais deve poder comprovar o consentimento dado pelo titular.

3.2.2 - Âmbito de Aplicação

3.2.2.1 - Aplicação Territorial

No âmbito da aplicação territorial, o RGPD aplica-se ao "tratamento de dados pessoais efetuado no contexto das atividades 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". [106]

Devido à dimensão da sua aplicação, o RGPD envolve todas as entidades dentro da UE assim como fora desta, cujas atividades estejam ligadas à "oferta de bens ou serviços a esses titulares de dados na União, independentemente da exigência de os titulares dos dados procederem a um pagamento" ou ao " controlo do seu comportamento, desde que esse comportamento tenha lugar na União". [107]

Por outras palavras, mesmo não estando localizada na União, se o processo de recolha e tratamento tratar dados de residentes da UE, a entidade deverá cumprir o regulamento.

3.2.2.2 - Aplicação Material

Em termos de aplicação material, o RGPD aplica-se ao "tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos em ficheiros ou a eles destinados" [108].

Desta forma, o RGPD é aplicável em quaisquer tratamentos de dados pessoais, sendo ou não automatizados, abrangendo assim, materialmente, quaisquer entidades que operem com dados pessoais.

[104] (Barreto, 2020)
[105] Art. 4º nº11 do RGPD
[106] Art. 3º nº1 do RGPD
[107] Art. 3º nº2 do RGPD
[108] Art. 2º nº1 do RGPD

3.2.3 - Direitos dos Titulares de Dados

3.2.3.1 - Direito de Transparência das informações, das comunicações e das regras para exercício dos direitos dos titulares dos dados

Tal como referido anteriormente, o RGPD é regido por um princípio de transparência que certifica que os dados recolhidos e consequente tratamento seja de fácil acesso e compreensão para o titular. O art.º 12º do RGPD expõe as regras para a aplicação deste princípio, que serão levadas a cabo pelo responsável pelo tratamento de dados e subcontratantes. Nesse sentido, estes estão comprometidos aos pressupostos do referido artigo[109].

3.2.3.2 - Direito à Informação e Acesso

Este direito à Informação e Acesso vem consagrado no RGPD nos artigos 13º, 14º e 15º. Aqui o regulamento estipula este direito enquanto *"o direito de obter do responsável pelo tratamento a confirmação de que os dados pessoais que lhe digam respeito são ou não objeto de tratamento e, se for esse o caso, o direito de aceder aos seus dados pessoais"* [110].

Deste modo, o titular dos dados deverá sempre poder ter acesso, fácil e gratuito, aos dados que lhe digam respeito e deve ser sempre informado aquando alguma transferência de dados, violação de segurança, entre outros.

3.2.3.3 - Direito à Retificação e ao Apagamento dos Dados Pessoais

O direito à retificação, consagrado no art.º 16º do RGPD, estipula que o titular "tem o direito de obter, sem demora injustificada, do responsável pelo tratamento a retificação dos dados pessoais inexatos que lhe digam respeito"[111].

Desta forma, o titular poderá retificar "dados pessoais inexatos que lhe digam respeito" junto da entidade, através de uma declaração adicional, quando entender que tal informação, pela sua imprecisão ou incongruência, consiga danificar eventuais ações futuras.

O direito ao apagamento dos dados pessoais, ou o "direito a ser esquecido" como é mais comummente conhecido, está estabelecido no art.º 17º do RGPD enquanto "o direito de obter do responsável pelo tratamento o apagamento dos seus dados pessoais, sem demora injustificada, e este tem a obrigação de apagar os dados pessoais, sem demora injustificada, quando se aplique um dos motivos"[112], esclarecidos no nº 1 do mesmo artigo.

Este é um reforço dos direitos dos titulares de dados, dotando-os de um maior controlo sobre os seus dados e centralizando-se no seu consentimento. Tal como referimos anteriormente, as entidades devem estar dotadas de mecanismos que permitam esta retificação ou até mesmo apagamento de dados, de forma a obedecer aos termos legais impostos pelo RGPD.

[109] art.º 12º do RGPD
[110] Art. 15º do RGPD
[111] Art. 16º do RGPD
[112] Art. 17º nº1 do RGPD

3.2.3.4 - Direito à limitação do tratamento

O direito à limitação do tratamento, explanado no art.º 18º do RGPD, trata de dotar o titular do poder de *"obter do responsável pelo tratamento a limitação do tratamento".* Este direito aplica-se quando o titular *"contestar a exatidão dos dados pessoais"*, *"solicitar a limitação da utilização dos dados"*, *"requirir os dados para efeitos de declaração, exercício ou defesa de um direito"* ou *"se opuser ao tratamento dos dados"* predisposto pela entidade[113].

Desta forma, o titular pode exigir à entidade que os seus dados sejam limitados de acordo com os seus interesses ou para que não sejam utilizados para outros fins.

3.2.3.5 - Direito à Portabilidade de Dados

O direito à Portabilidade de Dados, consagrado no art.º 20º do RGPD, refere-se "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"*[114]*.

Neste sentido, este direito confere ao titular dos dados a possibilidade de aceder aos seus dados e solicitar a sua transferência para outro serviço ou responsável, sempre que exista expresso consentimento ou sempre que o tratamento dos dados seja efetuado de forma automatizada.

Assim, tal como para a retificação e para o apagamento dos dados pessoais, é exigido às entidades que tenham mecanismos que permitam e facilitem esta potabilidade de dados.

3.2.3.6 - Direito à Oposição e Decisões Individuais Automatizadas (*profiling*)

O direito à oposição e decisões individuais automatizadas é apontado nos artigos 21º e 22º do RGPD.

O titular dos dados tem o *"direito de se opor a qualquer momento, por motivos relacionados com a sua situação particular, ao tratamento dos dados pessoais que lhe digam respeito, incluindo a definição de perfis ou «profiling» com base nessas disposições"* [115].

Assim como também tem o direito de *"não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar"* [116].

Desta forma, o RGPD veio instituir um novo modelo quanto ao tratamento automatizado, um processo cada vez mais importante para as empresas no contexto digital, dando aos titulares de dados a possibilidade de "*manifestar a sua opinião, contestar a decisão e solicitar que essa decisão tomada pelo algoritmo seja revista por uma pessoa*" [117].

[113] Art. 18º do RGPD
[114] Art. 20º nº1 do RGPD
[115] Art. 21º nº1 do RGPD
[116] Art. 22º nº1 do RGPD
[117] (Working Party 243, 2017)

3.2.4 - Responsabilidade pelo Tratamento

3.2.4.1 - Responsabilidade pelo Tratamento dos Dados

Segundo os artigos 24º e 18º do RGPD, cabe ao responsável ou responsáveis pelo tratamento dos Dados, ou aos subcontratantes designados, aplicar *"as medidas técnicas e organizativas que forem adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade com o presente regulamento".*[118]

O responsável pelo tratamento dos Dados poderá contratar subcontratantes *"que apresentem garantias suficientes de execução das medidas"*[119]. Contudo, o subcontratante não pode contratar outro subcontratante sem a autorização prévia do responsável pelo tratamento.[120] O mesmo se aplica ao tratamento dos dados, não podendo um "*subcontratante ou qualquer pessoa, que tenha acesso a dados pessoais*" proceder ao tratamento desses dados exceto por instrução do responsável pelo tratamento[121].

Estipulado pelo art.º 30º do RGPD, o responsável é obrigado pelo regulamento a preservar *"um registo de todas as atividades de tratamento sob a sua responsabilidade".* Deste registo, devem constar informações como o nome e contacto do ou dos responsáveis pelo tratamento, as finalidades do tratamento, um descritivo das categorias de titular e dos respetivos dados pessoais, categorias de destinatários a quem os dados pessoais foram ou serão divulgados, transferências dos dados para países terceiros ou organizações internacionais, prazos previstos para o apagamento dos dados e um descritivo das medidas técnicas e organizativas relativas à segurança.[122]

3.2.4.2 - Encarregado de Proteção de Dados

No caso de o tratamento ser realizado por um organismo público, por um responsável cuja atividade consista em operações de tratamento de dados pessoais em grande escala que exijam um controlo regular ou que consistam em operações de tratamento de categorias especiais de dados, deverá ser nomeado um Encarregado de Proteção de Dados (EPD) ou *Data Protection Officer (DPO)* [123].

No entanto, a posição do EPD distingue-se das funções do responsável e do subcontrante, dado que apenas coopera com a organização no que diz respeito ao tratamento dos dados pessoais.

Assim, este demarca-se da responsabilidade pelo tratamento, que cabe, tal como referido anteriormente ao responsável e ao subcontratante. E em caso de violação de dados pessoais, a entidade não poderá penalizar nem destituir o EPD[124].

No meio organizacional, as funções do EPD, referidas no art.º 39º do RGPD, passam por verificar o cumprimento do RGPD dentro da entidade, prestar informações à entidade acerca das suas obrigações, aconselhar e recomendar medidas relativas ao tratamento dos dados

[118] Art. 24º nº1 do RGPD
[119] Art. 28º nº1 do RGPD
[120] Art. 28º nº2 do RGPD
[121] Art. 29º do RGPD
[122] Art. 30º nº1 do RGPD
[123] Art. 37º do RGPD
[124] Art. 38º nº3 do RGPD

pessoais, cooperar com a autoridade de controlo e ainda estabelecer um ponto de contacto entre a autoridade de controlo e a entidade [125].

Relativamente às suas qualidades profissionais, referidas no art. 38º do regulamento, o EPD *"é designado com base nas suas qualidades profissionais e, em especial, nos seus conhecimentos especializados no domínio do direito e das práticas de proteção de dados, bem como na sua capacidade para desempenhar as funções referidas no art.º 39º"* [126].

No que diz respeito as suas competências especializadas, o EPD deverá possuir "*competências no domínio das normas e práticas de proteção de dados nacionais e europeias, incluindo um conhecimento profundo do RGPD; conhecimento das operações de tratamento efetuadas; conhecimento das tecnologias da informação e da segurança dos dados; conhecimento do setor empresarial e da organização; capacidade para promover uma cultura de proteção de dados na organização*"[127].

Com isto, o RGPD veio estabelecer um nível de preparação para as entidades, na matéria de proteção de dados, e nomear um EPD, caso seja necessário. Não obstante, o RGPD não impede de outras entidades procurarem aconselhamento junto de um EPD relativamente a matérias que concernem a proteção de dados.

3.2.4.3 - Proteção de Dados por conceção (*Privacy by Design*) e Proteção de Dados por Defeito (*Privacy by Default*)

As "medidas técnicas e organizativas" apresentadas no art.º 24º do RGPD, podem ter dois meios de aplicação considerando "as técnicas mais avançadas, os custos da sua aplicação, e a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos decorrentes do tratamento para os direitos e liberdades das pessoas singulares"[128].

Estas duas formas de aplicação são expostas no art.º 25º do RGPD, como a proteção de dados por conceção e por defeito.

A Proteção de dados por conceção ou "Privacy by Design" consiste na aplicação de táticas, "tanto no momento de definição dos meios de tratamento como no momento do próprio tratamento", oportunas para a aplicação eficaz dos princípios expostos anteriormente, assim como a inclusão das garantias fundamentais para o tratamento [129].

Desta forma, o responsável pelo tratamento deverá assegurar, no momento de recolha dos dados, estes são tratados de acordo com o regulamento e com os direitos enunciados por todos eles.

A Proteção de Dados por defeito ou "Privacy by Default" estipula que apenas "sejam tratados os dados pessoais que forem necessários para cada finalidade do tratamento". Ou seja, o responsável de tratamento de dados pessoais, apenas recolhe os dados necessários durante um

[125] Art. 39º nº1 do RGPD
[126] Art. 37º nº5 do RGPD
[127] (Working Party 243, 2017)
[128] Art. 25º nº1 do RGPD
[129] Art. 25º nº1 do RGPD

certo período de conservação e com acessibilidade limitada de forma a que "não sejam disponibilizados sem intervenção humana a número indeterminado de pessoas singulares"[130].

3.2.4.4 - Segurança do Tratamento dos Dados

Tal como referido anteriormente, as entidades devem aplicar *"medidas técnicas e organizativas"* que assegurem um determinado nível de segurança contra ameaças, como violações de dados pessoais.

Previsto no art.º 32º do RGPD, tais medidas deverão incluir a pseudonimização dos dados, a capacidade de assegurar a confidencialidade e integridade dos serviços de tratamento, a capacidade de acesso aos dados pessoais *"em caso de incidente físico ou técnico"*, assim como um mecanismo de avaliação da eficácia destas medidas[131].

Desta forma, o regulamento apresenta um reforço nas medidas a tomar em caso de violação de dados pessoais, que se seguem com a notificação[132] e comunicação[133] da mesma ao titular dos dados pessoais e a autoridade de controlo competente.

O responsável pelo tratamento dos dados deverá proceder a esta notificação até 72 horas, após ter conhecimento dela. Esta notificação deverá conter um descritivo da natureza da violação, o nome e contacto do EDP, as potenciais consequências da violação e um descritivo das medidas adotadas para proceder à reparação ou atenuar possíveis repercussões[134].

Salvaguardado pelo art.º 34º do RGPD, em caso de violação de dados, o responsável deverá também comunicar o incidente ao titular dos dados pessoais *"sem demora injustificada"* e *"em linguagem clara e simples"* [135].

3.2.4.5 - Avaliações de Impacto

Consagrado no art.º 35º do RGPD, as avaliações de impacto surgem aquando a utilização de novas tecnologias que impliquem *"elevado risco para os direitos e liberdades das pessoas singulares"* [136].O Responsável pelo tratamento, aquando esta avaliação sobre a proteção de dados, poderá solicitar um parecer do EDP[137].

Também no referido artigo, o RGPD prevê alguns exemplos de quando é que é necessário realizar uma avaliação de impacto, nomeadamente. Cabe ao responsável pelo tratamento elaborar guias de boas práticas relativas ao tratamento de dados pessoais[138].

Contudo, não é estabelecida uma metodologia comum, podendo as entidades publicar, cada uma, as suas próprias metodologias, desde que cumpram os critérios do RGPD.

[130] Art. 25º nº2 do RGPD
[131] Art. 32º nº1 do RGPD
[132] Art. 33º nº1 do RGPD
[133] Art. 34 nº1 do RGPD
[134] Art. 33º nº3 do RGPD
[135] Art. 34º nº1 do RGPD
[136] Art. 35º nº1 do RGPD
[137] Art. 35º nº2 do RGPD
[138] Art. 35º nº7 do RGPD

3.2.5 - Transferência de Dados Pessoais

3.2.5.1 - Princípio Geral das Transferências

De acordo com o art.º 44º do RGPD, transferências de dados pessoais para países terceiros ou organizações internacionais apenas poderão ser realizadas, se forem respeitadas as condições estabelecidas pelo regulamento, que asseguram *"que não é comprometido o nível de proteção das pessoas singulares"* [139].

Nesse sentido, transferências de dados pessoais para um país terceiro ou uma organização internacional só poderão ser realizadas se a Comissão Europeia tiver decidido que o país ou organização em questão garantem um *"nível de proteção adequado"* [140].

Esta avaliação do nível de proteção é feita tendo em conta os seguintes fatores[141]:

- Respeito pelo Estado de Direito, Direitos Humanos e liberdades fundamentais, assim como, existência e aplicação de legislação pertinente;
- Existência de uma ou mais autoridades de controlo independentes no país terceiro ou às quais está sujeita uma organização internacional;
- Compromissos internacionais assumidos pelo país terceiro ou pela organização internacional, relativos à proteção de dados pessoais;

Após esta avaliação, a CE poderá decidir, favorável ou desfavoravelmente, no que diz respeito ao nível de proteção assegurado pelo país terceiro ou organização internacional. Sendo que, se positivo, realizar-se-á uma "*avaliação periódica, no mínimo de quatro em quatro anos, que deverá ter em conta todos os desenvolvimentos pertinentes no país terceiro ou na organização internacional"* [142].

No caso de não ter sido tomada qualquer decisão por parte da CE, os dados pessoais só podem ser transferidos para um país terceiro ou uma organização internacional, se forem apresentadas as garantias adequadas, e que, adicionalmente, os titulares dos dados possam usufruir de *"direitos e medidas jurídicas corretivas"* [143].

3.2.5.2 - Regras Vinculativas Aplicáveis às Empresas

Tal como explicado anteriormente, estas regras, consagradas no art.º 47º do RGPD, têm como objetivo o tratamento dos dados, durante uma transferência, de forma a que sejam cumpridas tanto por uma entidade sediada na UE, como também fora desta[144].

Se o nível de segurança não for adequado no país terceiro ou na organização internacional, a transferência dos dados deverá ser proibida.[145] Contudo, isto poderá ser suprido se forem respeitadas as normas do RGPD, as regras vinculativas e as derrogações para situações especiais, salvaguardadas no art.º 49º do regulamento.

---

[139] Art. 44º do RGPD
[140] Art. 45º nº1 do RGPD
[141] Art. 45º nº2 do RGPD
[142] Art. 45º nº3 do RGPD
[143] Art. 46º nº2 & 3 do RGPD
[144] Art. 47º do RGPD
[145] Art. 45º nº5 do RGPD

Empresas que tenham um sítio na internet, poderão divulgar as suas regras, de forma a dar conhecimento ao titular dos dados pessoais o que acontece aquando transferências de dados.

3.2.6 - Autoridade de Controlo Independente

3.2.6.1 - Estatuto, Competência, atribuições e poderes

Tal como explicado anteriormente nesta investigação, esta autoridade de controlo é uma autoridade pública independente, criada pelo respetivo Estado-Membro, cujo objetivo é controlar o cumprimento do RGPD, podendo para isso, cooperar com outras autoridades de controlo.

Estas autoridades, tal como está consagrado no RGPD, operam com total independência[146] e são livres de *"influências externas, diretas ou indiretas"*[147], de forma a exercerem as suas atribuições e poderes, salvaguardados nos artigos 57º e 58º.

Estas organizações têm competência para tratar de qualquer reclamação que lhes sejam apresentadas ou para tratar de eventuais violações do regulamento, se estiverem relacionadas com uma entidade localizada ou se afetar *"substancialmente"* titulares dos dados no respetivo Estado-Membro[148].

A constituição destas autoridades de controlo está dependente dos pressupostos do art.º 54.º do RGPD. Os membros das autoridades são escolhidos de acordo com as suas "habilitações, a experiência, conhecimentos técnicos necessários [...] no domínio da proteção de dados pessoais" [149].

3.2.7 - Vias de Recurso e Sanções

3.2.7.1 - Direitos

Além dos direitos já apresentados nesta análise, em caso de violação de dados, os titulares dispõem de ações jurídicas, as quais podem recorrer em defesa dos seus direitos.

O RGPD possibilita aos titulares de dados recorrer a uma autoridade habilitada no âmbito dos dados pessoais, assim como também apresenta a possibilidade de apresentar uma ação judicial[150] ou reclamação[151] contra uma autoridade de controlo, se a mesma *"não tratar a reclamação ou não informar o titular dos dados, no prazo de três meses, sobre o andamento ou o resultado da reclamação"* [152].

Adicionalmente, o titular de dados poderá também apresentar uma ação judicial contra um responsável pelo tratamento ou um subcontratante, se considerarem *"ter havido violação de*

[146] Art. 52ª nº1 do RGPD
[147] Art. 52º nº2 do RGPD
[148] Art. 55º nº1 do RGPD
[149] Art. 53º nº2 do RGPD
[150] Art. 78º nº1 do RGPD
[151] Art. 77º nº1 do RGPD
[152] Art. 78º nº2 do RGPD

direitos, na sequência do tratamento dos seus dados pessoais efetuado em violação do referido regulamento" [153].

No que diz respeito à representação do titular, o RGPD, no seu art.º 80, prevê que o titular tem o direito *"de mandatar um organismo, organização ou associação sem fins lucrativos",* cuja atividade incida sobre os direitos e liberdades dos titulares relativamente à proteção de dados pessoais[154].

Se, de facto, se verificar que o titular sofreu danos materiais ou imateriais por causa de uma violação do RGPD, o mesmo tem direito a receber uma indemnização do responsável pelo tratamento ou do subcontratante pelos danos sofridos[155].

Desta forma, o titular dos dados dispões de uma variedade de direitos que não só o protegem aquando o tratamento dos seus dados como também em caso de violação dos mesmos, com alternativas judiciais.

3.2.7.2 - Coimas

O RGPD, nos seus artigos 83º e 84º, estipula a aplicação de coimas e sanções, no caso de haver violações do regulamento. De acordo com o regulamento, as coimas poderão atingir, no limite, 20 000 000 de euros ou 4% do volume de negócios anual, se se tratar de uma empresa.[156] Contudo, o regulamento permite que os Estados-Membros, como Portugal, possam determinar quando e de que forma as coimas podem ser aplicadas no seu território, possibilitando assim uma maior flexibilidade e ajuste à realidade dos Estados-Membro.[157]

3.3 - Transposição para Portugal

Tendo em conta o que foi dito anteriormente, a relevância dada à privacidade e à proteção dos dados pessoais em Portugal é algo histórico e o desenvolvimento destes conceitos no espectro jurídico português foi evoluindo a par com a sua Lei Fundamental, a CRP. Nesse sentido, e observando a aplicação do RGPD, através daquilo que chamamos LNPD, podemos afirmar que a transposição do regulamento europeu para Portugal criou algumas regras mais específicas e alguns complementos aos pontos mais gerais[158].

3.3.1 - Comissão Nacional de Proteção de Dados

Tal como estipulado pelo RGPD, é necessária a criação de autoridade de controlo pública e independente, de forma a aplicar o regulamento europeu em território nacional português. A LNPD estipula que a CNPD é a autoridade de controlo nacional responsável pela aplicação do RGPD em Portugal[159].

Todas as entidades públicas e privadas, de acordo com o âmbito de aplicação da LNPD, deverão colaborar com o CNPD, aquando necessário para a realização das suas funções. Estipulando assim um dever de colaboração entre as entidades e a CNPD, desde que não afetem

[153] Art. 79º nº1 do RGPD
[154] Art. 80º nº1 do RGPD
[155] Art. 82º nº1 do RGPD
[156] Art. 83º nº6 do RGPD
[157] Art. 83º nº7 do RGPD
[158] (Lei n.º 58/2019, 2019)
[159] Art. 3º da LNPD

o dever de sigilo profissional, nos termos do art.º 54º do RGPD, ao qual o responsável pelo tratamento está sujeito[160].

Além das atribuições expostas no RGPD, a LNPD vai mais longe, consagrando à CNPD o poder de, nos termos do art.º 6º:

- Emitir pareceres sobre medidas legislativas e/ou regulamentares quanto à proteção de dados pessoais;
- Corrigir e sancionar o incumprimento do regulamento;
- Disponibilizar uma lista de tratamentos sujeitos a avaliação de impacto sobre a proteção de dados;

3.3.2 - Responsabilidade

No que diz respeito à responsabilidade pelos dados, o LNPD segue a mesma linha do RGPD, definindo critérios para a nomeação de EPD tanto para entidades públicas[161], como privadas[162], consagrados nos artigos 12º e 13º da LNPD. Porém, a lei nacional vai mais longe do que RGPD em termos das funções do EPD, às quais acresce a realização de auditorias, criação de ações de sensibilização junto dos utilizadores e manter relações com os titulares de dados[163].

3.3.3- Coimas, Crimes e Sanções

A LNPD distingue entre duas categorias de infrações: as contraordenações muito graves[164] e as contraordenações graves[165], respetivamente consagradas nos artigos 37º e 38º. São estipuladas coimas para ambas estas eventualidades.

No que diz respeito às contraordenações muito graves para grandes empresas, as coimas vão de 5 mil a 20 Milhões de euros ou 4% do volume de negócios anual, sendo aplicada a penalização mais alta. Para as PME, a coima estende-se entre os 2 mil e os 2 milhões de euros ou também 4% do volume de negócios anual. Em caso de pessoas singulares, a punição tem um mínimo de mil euros e um máximo de 500 mil euros.[166]

No que toca às contraordenações graves, para grandes empresas a coima está entre os 2500 euros e os 10 milhões de euros ou 2% do volume de negócios anual. Para as PME, a coima é também ou 2% do volume de negócios anual ou estará entre os mil e 1 milhão de euros. Para pessoas singulares, a coima fica entre os 500 e os 250 mil euros[167].

Estas coimas são determinadas de acordo com a situação económica do agente ou o seu volume de negócios, no caso de uma empresa, o caráter da infração e a dimensão da entidade em causa[168]. Dessa forma, estas multas prescrevem após 2 anos caso sejam contraordenações graves ou o montante sejam iguais ou inferiores a 100 mil euros[169] ou após 3 anos, caso

[160] Art. 4º da LNPD
[161] Art. 12º da LNPD
[162] Art. 13º da LNPD
[163] Art. 13º da LNPD
[164] Art. 37º da LNPD
[165] Art. 38º da LNPD
[166] Art. 37º da LNPD
[167] Art. 38º da LNPD
[168] Art. 39º da LNPD
[169] Art. 40º da LNPD

consistam em contraordenações muito graves ou o montante seja superior a 100 mil euros.[170] O montante das coimas cobradas reverte em 60% para o Estado e em 40 % para a CNPD[171].

No que diz respeito ao espetro criminal da LNPD, é considerado crime a utilização de dados de forma incompatível com a finalidade de recolha[172], o acesso indevido[173] e desvio de dados[174], assim como a violação do dever de sigilo[175] ou de obediência[176]. Estas infrações são punidas com pena de prisão até 1 ano ou com pena de multa até 120 dias, podendo ser agravadas se se tratar de categorias especiais de dados, consagrados nos artigos 9º e 10º do RGPD.

A viciação ou destruição de dados[177] e a inserção de dados falsos[178], com intuito de causar prejuízo, são punidas, por sua vez, com pena de prisão até 2 anos ou pena de multa até 240 dias. Estas penas poderão ser agravadas se resultar das infrações algum dano especialmente grave e efetivo.

Além destas punições, poderão aplicadas outras sanções, nos termos do art.º 56º da LNPD, tais como a proibição temporária ou definitiva do tratamento, o bloqueio, o apagamento ou a destruição total ou parcial dos dados[179]. Se se tratar de um crime ou coima superior a 100 mil euros, poderá ser publicitada a condenação no Portal do Cidadão por um período igual ou superior a 90 dias, com *"a identificação do agente, os elementos da infração e as sanções aplicadas"* [180].

3.3.4 - Outras Disposições

Salvo todas os complementos já apresentados, a LNPD estipula que a idade mínima para o consentimento de utilização de dados pessoais é de 13 anos inclusive. Inferior a esta idade, o tratamento só é lícito se for consentido pelos representantes legais da criança[181].

Além disso, a videovigilância é permitida, nos termos do art.º 19º da LNPD, contudo a captação de som é proibida, exceto quando as instalações estão encerradas ou existe autorização prévia da CNPD[182].

[170] Art. 41º da LNPD
[171] Art. 42º da LNPD
[172] Art. 46º da LNPD
[173] Art. 47º da LNPD
[174] Art. 48º da LNPD
[175] Art. 51º da LNPD
[176] Art. 52º da LNPD
[177] Art. 49º da LNPD
[178] Art. 50º da LNPD
[179] Art. 56º nº1 da LNPD
[180] Art. 56º nº2 da LNPD
[181] Art. 13º da LNPD
[182] Art. 19º da LNPD

Capítulo IV – Proteção de Dados Pessoais no Retalho Omnicanal

Tal como podemos verificar anteriormente, esta legislação teve um impacto direto tanto em negócios como na vida dos cidadãos europeus, incluindo também instituições governamentais e intergovernamentais.

Para um cidadão de um Estado-Membro da UE, este regulamento melhora significativamente os seus direitos na esfera digital, dependendo sempre da adesão da empresa às políticas de proteção de dados. Considerando que os utilizadores apenas interagem com retalhistas que respeitam o RGPD, este confere-lhes uma série de direitos já enunciados anteriormente.

Em contrapartida, as opções para os retalhistas que operam na UE são limitadas à adoção ou à não-adoção do regulamento. Ao introduzir este regulamento, primeiro, as empresas precisaram de se preparar, dado que este apresenta alterações à forma como as entidades gerem e processam dados.

4.1 - O Papel dos Dados Pessoais no Retalho Omnicanal

Os dados são o centro de toda a atividade da empresa [183]. A utilização dos dados pessoais permite um maior conhecimento sobre quem é o cliente e, consequentemente, uma melhor experiência de compra. A principal característica do retalho omnicanal centra-se no facto de ser uma estratégia que se foca no consumidor de forma a oferecer-lhe uma experiência "holística"[184] [185].

O retalho tradicional já se focava em armazenar produtos que o seu público-alvo irá gostar (logística e cadeia de abastecimento), gerar conhecimento sobre o que é vendido na loja (marketing) e, posteriormente, facilitar o processo de compra (experiência de compra)[186].

No mundo do omnicanal, os dados pessoais permitem ir muito além desta estratégia. No que diz respeito à experiência de compra, utilizando os dados pessoais, é possível aos retalhistas enviar cupões e ofertas aos clientes através dos seus dispositivos *mobile*. Assim como também oferecer promoções consoante a localização do consumidor [187].

Os dados recolhidos dos consumidores e dos *stakeholders* é a espinha dorsal de qualquer operação logística. A estratégia omnicanal, garantindo a integração dos canais disponíveis, por sua vez, garante o fluxo de dados através de toda a cadeia de abastecimento. Dessa forma, *"os dados são entregues ao recipiente apropriado, na altura certa e na quantidade adequada"* [188].

Consequentemente, com melhor acesso aos dados, permite mais flexibilidade dentro da cadeia de abastecimento entre fabricantes, retalhistas e empresas de logística de forma a que haja entregas mais dinâmicas, uma maior satisfação do cliente e opções de entrega mais diversificadas [189].

[183] (CrowdFlower, 2017)
[184] (Gupta, Lehmann, & Stuart, 2004)
[185] (Shah, Rust, Parasuraman, Staelin, & Day, 2006)
[186] (Rigby, 2011)
[187] (Rigby, 2011)
[188] (Weilland, 2016)
[189] (Dalsey Hillblom Lynn, 2020)

4.2 - Impactos do RGPD no Retalho Omnicanal

A aplicação do RGPD numa entidade começa no momento em que desenhamos um produto até ao momento em que processamos os dados. Sem exceção, no retalho omnicanal, a aplicação do regulamento acontece desde o momento de extração do recurso até a entrega do produto ao cliente.

4.2.1- Impactos no Processo de Recolha e Tratamento de Dados

A recolha e o tratamento de Dados Pessoais são essencias para a prosperidade de um negócio. Quanto mais informação a empresa tiver acerca dos seus consumidores, melhor poderá formular a sua mensagem e o seu produto às suas necessidades e expectativas. A implementação do RGPD levantou questões relativas à recolha e ao tratamento de dados pessoais, impactando todos os métodos utilizados para este objetivo.

Nesse sentido, podemos dividir este processo em 4 processos diferentes: em primeiro lugar, o processo de recolha, onde as entidades procedem à recolha dos dados junto dos titulares de dados. O segundo processo consiste na consolidação de mecanismos de segurança que as entidades devem ter para proteger os dados sobre os quais têm controlo. Em terceiro lugar, surge o processo de controlo, onde as entidades operacionalizam os direitos dos Titulares de Dados consagrados pelo RGPD. Posteriormente, o processo de comunicação trata do diálogo entre entidades e Titulares de Dados, no caso de ser necessária uma notificação ou quando existe uma violação de dados referentes ao Titular dos Dados [190].

Dessa forma, neste subcapítulo, podemos observar de que forma o regulamento mudou a recolha de dados pessoais, o método de os proteger e ainda adicionou duas novas etapas, nomeadamente de controlo e comunicação.

4.2.1.1 - Processo de Recolha de Dados Pessoais

4.2.1.1.1- Rastreio Online

O rastreio online é um processo de recolha e partilha de informações sobre as atividades de um indivíduo na *web*. As empresas utilizam uma série de instrumentos para observar como o utilizador interage com a plataforma, seja ela um *website* ou uma aplicação *mobile*. Dos instrumentos mais utilizados para realizar estas tarefas, destacam-se os HTTP *cookies* e o rastreio por endereço IP [191].

Os *cookies* são pedaços de código que são colocados navegador de um utilizador sempre que este utiliza um website que os usa. Estes servem para informar o website sobre o comportamento do utilizador de forma a criar uma experiência o mais personalizada possível. Contudo, poderão ser também utilizados por terceiros para o histórico de navegação do utilizador, por exemplo no caso da publicidade online, onde se pretende rastrear o tráfego de anúncios colocados noutros *websites* [192].

O endereço IP é uma série de números que identifica o dispositivo do utilizador na *internet*. Todos os dispositivos dispõem de um endereço IP, e, dessa forma, consegue indicar a

[190] Art. 33º e 34º do RGPD
[191] (Belcic, 2021)
[192] (DMN News, 2018)

localização física do utilizador. Assim, ao utilizar o rastreio por endereço IP, as entidades conseguem perceber de onde está o utilizador e formar padrões de comportamento para prever os seus padrões de consumo [193].

A discussão relativamente à utilização de *cookies* e a proteção da privacidade dos Titulares data de 2011. Contudo, a introdução do RGPD estipulou que identificadores digitais como o endereço IP e os *Cookies* são também considerados dados pessoais [194].

Não obstante, mesmo enquanto dados pessoais não-sensíveis, estão submetidos ao regulamento europeu e aos seus princípios e direitos já enunciados. Ou seja, deverão ser recolhidos com o consentimento dos Titulares de Dados, sendo o ato de tratamento dos dados antes do consentimento punível pela lei em vigor [195].

4.2.1.1.2 - Marketing Analytics

As métricas de *Analytics* referem-se às estatísticas da performance do website e como o utilizador o utiliza. Visto que é um processo que implica instrumentos de rastreio *online* como *cookies* e endereços de IP, o consentimento do utilizador é necessário. Além disso, a utilização de *softwares* de terceiros para realizar este processo, como por exemplo o Google Analytics, dependendo do acordo estabelecido com a entidade terceira, requer que os responsáveis pelo tratamento de dados informem os Titulares que os seus dados estão a ser enviados para essa entidade, podendo esta ser dentro ou fora da EU [196].

4.2.1.1.3- Monitorização das Redes Sociais

A monitorização das redes sociais refere-se à utilização das redes sociais para a monitorização, recolha e extração de dados. Embora os impactos do RGPD nas redes sociais não sejam os mais claros, estes existem sobretudo na área da publicidade paga e em 2 principais vertentes, anúncios de *remarketing* e rastreio comportamental [197].

Em termos de *remarketing*, com o RGPD, a utilização deste tipo de anúncios requer que os consumidores tenham aceite o uso dos seus dados para esse fim [198]. Isto impacta o processo dado que acrescenta mais passos à realização de campanhas nas redes sociais e oferece aos consumidores mais oportunidades de querer sair do processo [199].

Relativamente ao rastreio comportamental, a utilização de ferramentas de análise de redes sociais permite às entidades saber mais sobre os seus visitantes e se os seus anúncios estão a ter um ROI adequado [163]. Com o RGPD, o rastreio comportamental dos visitantes das redes sociais das entidades é mais limitado. Contudo, as próprias entidades que gerem os instrumentos de análise, como o Facebook, já aplicaram o RGPD de forma a que o seu produto possa fornecer conhecimento sobre o visitante [200].

[193] (Belcic, 2021)
[194] Art. 4º do RGPD
[195] (iubenda, 2020)
[196] (Besemer, 2018)
[197] (Geyser, 2021)
[198] (Unbox Social, 2018)
[199] (Geyser, 2021)
[200] (Unbox Social, 2018)

4.2.1.1.4 - Dados de Subscrição e /ou Inscrição

Relativamente a dados de subscrição e inscrição, por exemplo, quando um utilizador na UE subscreve a um serviço. Se a entidade quiser utilizar esses dados, como por exemplo o e-mail do titular de dados, terá *a priori*, no momento de recolha de dados, obter permissão por parte do titular de dados para que possa proceder ao tratamento dessas informações [201].

Posteriormente, esse consentimento deverá ser demonstrável, de uma forma concisa e transparente, ou seja, se a entidade que supervisiona a aplicação do RGPD pedir essa informação, entidades com serviços de subscrição deverão preservá-la [202].

4.2.1.2 - Processo de Segurança dos Dados

A implementação do RGPD veio trazer mudanças significativas relativamente ao processamento e à segurança dos dados. A partir da sua aplicação, o RGPD tornou necessária a inclusão de terceiros relevantes na auditoria relativa ao cumprimento do regulamento. Adicionalmente, a legislação introduz às empresas os já referidos novos processos de forma a dificultar a identificação dos titulares de dados.

A Segurança dos Dados está historicamente conectada à ideia de confidencialidade, ou seja, os dados são acessíveis apenas a entidades autorizadas, garantindo assim a sua segurança[203]. Além deste, existem outros princípios que devem ser considerados para a proteção dos dados e informações. Para Sêmola, os três princípios fundamentais para implementar mecanismos de segurança dos dados são a confidencialidade, a integridade e a disponibilidade. A integridade é definida pelo autor como a não-alteração dos dados por entidades não autorizadas pelo seu titular, ao passo que a disponibilidade trata que a informação deverá estar disponível sempre que necessária [204].

Adicionalmente, Nakamura e Geus acrescentam dois princípios para o alcance da segurança dos dados, sendo estes a autenticidade e o não-repúdio ou irretratabilidade. A autenticidade explica que os dados e as informações, sendo verdadeiros deverão anunciar a sua fonte. Por outro lado, a irretratabilidade trata da garantia que *"uma entidade não negue a autoria de algo realizado por ela*" [205].

Por fim, Demétrio apresenta o princípio da tempestividade, que se debruça sobre a garantia de validade de informação nos documentos eletrônicos ao longo do tempo[206]. Para cada um destes princípios apresentados são aplicados mecanismos específicos tecnológicos, tal como podemos ver na figura 2.

[201] Art. 7º nº1 do RGPD
[202] (Vilumns, 2018)
[203] (Freund, Fagundes, Macedo, & Dutra, 2019)
[204] (Sêmola, 2014)
[205] (Nakamura & Geus, 2007)
[206] (Demétrio, 2003)

Figura 8 - Mecanismos tecnológicos da segurança da informação

MECANISMO DE SEGURANÇA	DESCRIÇÃO
Criptografia	Possui importância fundamental para a segurança da informação, uma vez que é a base para diversas tecnologias e protocolos utilizados com objetivo de garantir confidencialidade, integridade, autenticação e irretratabilidade das informações. Este mecanismo transforma dados legíveis em ilegíveis utilizando um código de maneira que somente entidades autorizadas e detentoras do mesmo conseguem descriptografá-los e interpretá-los (NAKAMURA; GEUS, 2007).
Hashing	São cálculos matemáticos utilizados em algoritmos que produzem o histórico da informação possibilitando identificar se a mesma foi alterada. Algoritmos de cálculo de *hashing* são usados para garantir a integridade e identificar se ocorreram mudanças não previstas. (MORAES, 2010).
Assinatura digital	É a combinação de mecanismos de *hashing* e criptografia, utilizada para garantir a autenticidade, a integridade e a irretratabilidade da informação (MORAES, 2010).
Controle de acesso	Trata da limitação de acesso às informações e deve ser implementado considerando a "necessidade de conhecer" e a "necessidade de acesso". A norma recomenda que as permissões de acesso sejam aprovadas pelo responsável pela informação. Além disso, o recurso de "perfil" pode ser adotado para autorizar não somente os acessos, mas também as ações individuais ou de um grupo de usuários (ISO/IEC 2002:2013).
Backup	São cópias de segurança que garantem a recuperação das informações em caso de perda ou indisponibilidade das mesmas em suas bases originais (ISO/IEC 2002:2013).
Certificados Digitais	Materializam o uso da assinatura digital e possibilitam o uso da criptografia, sendo emitidos por autoridades certificadoras que atestam que as informações utilizadas em sua geração são verdadeiras e válidas por um determinado tempo. Com o uso de funções matemáticas é possível se obter garantia da autenticidade, irretratabilidade, integridade e confidencialidade (FONTES, 2008).
Carimbo de tempo	Garante a validade de uma informação assinada digitalmente ao longo do tempo. É um selo que atesta a data e a hora que um documento foi assinado digitalmente assegurando que o mesmo não foi adulterado no intervalo de tempo entre a assinatura e a consulta ao documento. Este mecanismo agrega uma âncora temporal ao documento eletrônico de forma que algumas características presentes em documentos físicos, como identificação de autoria e alteração no documento de forma imperceptível, também estejam presentes em documentos eletrônicos para evitar possíveis contestações jurídicas (DEMÉTRIO, 2003).

Fonte: (Freund, Fagundes, Macedo, & Dutra, 2019)

Tal como podemos observar na tabela acima representada, existem vários mecanismos de segurança que as empresas poderão implementar. Desde instrumentos para a autenticação do utilizador até troca de informações ou dados criptografados. Não obstante, o RGPD veio introduzir outros processos para garantir a segurança dos dados pessoais.

4.2.1.2.1 – Privacy by Design/Privacy by Default

Dentro do processo de *Privacy by Design*, as entidades são encorajadas a implementar processos e medidas, que visem a proteção dos dados dos utilizadores e consumidores, desde as primeiras fases da concepção das operações de tratamento. Por exemplo, a integração de processos como a anonimização e a pseudonimização, que serão explicados posteriormente, desde a fase de planeamento dos processos vai de acordo com o que o regulamento europeu exige às empresas [207]. Desta forma, a questão da privacidade é considerada desde o início da

[207] (European Comission, 2018)

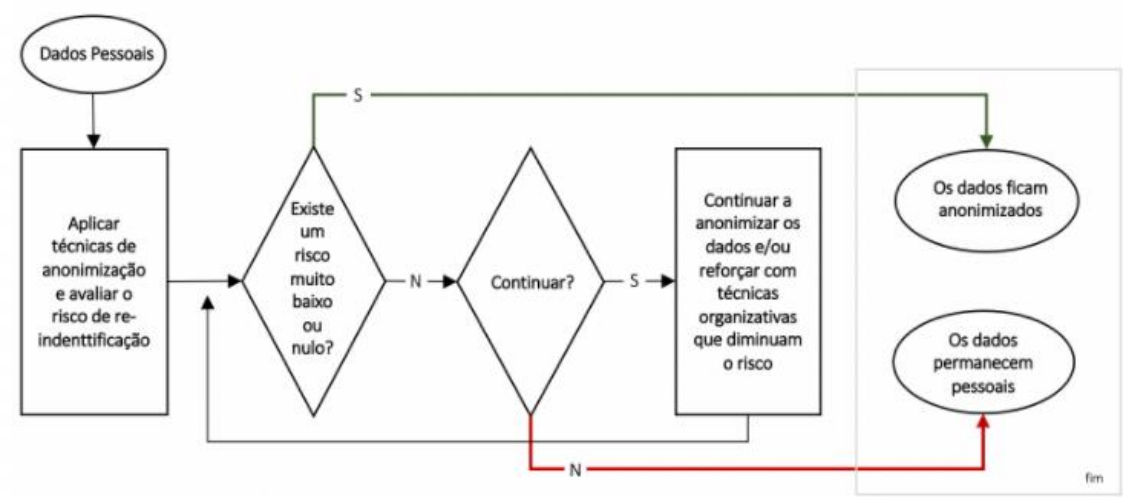
concepção de um produto ou serviço e não apenas um pensamento posterior ao processo de desenvolvimento [208].

No caso de um processo de *privacy by default*, as entidades devem assegurar que os dados são tratados com o mais elevado nível de proteção para que, por defeito, os dados não possam estar acessíveis a um número indefinido de pessoas [209]. Isto, por sua vez, poderá incluir avaliação de necessidade de dados, curtos períodos de armazenamento ou até mesmo acessibilidade limitada. Tendo isto em conta, a introdução destes dois novos conceitos pôs a privacidade como um ponto fundamental no desenvolvimento de um novo produto ou serviço. Apesar de impactar o processo de desenvolvimento, ao introduzir novas fases e custos, estes processos permitem às entidades pensarem, com antecedência, que tipo de dados pessoais necessitam, para que finalidade e como vão utilizá-los. Isto, por sua vez, torna o processo de desenvolvimento mais eficiente, visto que reduz a probabilidade de potenciais desafios, numa fase posterior [210].

4.2.1.2.2 – Anonimização

O Processo de Anonimização de Dados é uma *"técnica de processamento de dados que remove ou modifica informações que possam identificar uma pessoa"*. Este processo resulta em dados que não podem ser associados a nenhum Titular de Dados [211]**.** Através desta técnica é possível remover ou encobrir toda a informação pessoal de uma base de dados, de forma a impossibilitar ou tornar impraticável a identificação dos indivíduos[212].

Figura 9 – Processo de Anonimização



Fonte: (Universidade de Coimbra, 2021)[213]

O Processo de Anonimização dos dados deve ser implementado conjuntamente com uma estratégia de *"Privacy by Design".* Ou seja, em primeiro lugar identificar quais são os dados que são necessários para as respetivas finalidades. De seguida, a entidade aplica as técnicas de anonimização e verifica se existe algum risco, como por exemplo, re-identificação de dados pessoais. Se este risco não existir, os dados ficam anonimizados, contudo se o mesmo existir é

[208] (Danon, 2017)
[209] (European Comission, 2018)
[210] (ICO, 2018)
[211] (Machado & Doneda, 2018)
[212] (Pinho, 2017)
[213] Consultar website: https://www.uc.pt/protecao-de-dados/protecao_dados_pessoais/anonimizacao

necessário continuar aplicar técnicas organizativas até que o risco diminua para um nível nulo ou muito baixo.

Figura 10 - Exemplo de aplicação de Técnicas de Anonimização

Identificadores diretos ou singulares		Indicadores indiretos (semi-identificadores)			
ID	Nome	Idade	Género	Endereço	Telefone
1234...	José Maria...	21	Masculino	Rua Abc...	911 222 333
2345...	Manuel João...	32	Masculino	Rua Bcd...	921 333 444
3456...	Joana Manuel...	43	Feminino	Rua Cde...	931 444 555
4567...	Maria José...	45	Feminino	Rua Def...	941 555 666

Indentificadores diretos	Atributos* sensíveis		
ID	Conta	Tipo	saldo
1234	000504321	Ordem	10.123€
2345	000505432	ordem	20.234€
3456	000506543	ordem	20.345€
4567	000507654	ordem	10.345€

Fonte: (Universidade de Coimbra, 2021)

O processo de anonimização pode abranger técnicas como por exemplo, o encobrimento de caracteres, a substituição do valor de um atributo em vários registos, a substituição do atributo com informação não relacionada, mas coerente ou até mesmo a total remoção do atributo. Desta forma, este processo vai ao encontro dos direitos dos Titulares de Dados e minimiza o risco de quebra da privacidade. Não obstante este processo é apenas tão ou mais eficaz quanto menor for a possibilidade do Titular de Dados ser identificado.

4.2.1.2.3 - Pseudonimização

Ao contrário da anonimização, cujo objetivo é a de-identificação do Titular dos Dados, a pseudonimização procura fazer uma identificação, mas através de um disfarce que impede que a identificação real do utilizador seja revelada. Por outras palavras, esta técnica não remove informações de identificação dos dados, mas apenas substitui os identificadores pessoais por palavras ou códigos, o que torna os dados ininteligíveis. Desta forma, embora integre mais passos dentro do processo de segurança, a pseudonimização resulta numa redução dos riscos de exposição dos titulares de dados e possibilita segurança adicional para os responsáveis pelo tratamento [214].

4.2.1.2.4 – Gestão de Acessos

Segundo o regulamento, cabe à entidade "assegurar a confidencialidade, integridade, disponibilidade e resiliência […] dos sistemas". De forma a que isto se faça da forma mais eficiente possível, é necessário que exista um sistema de gestão de acessos que regule os acessos de cada colaborador [215].

Este sistema, por sua vez, garante que os dados apenas estão acessíveis a quem tem direito a aceder, que são exatos, que estão disponíveis sempre que necessário e que são totalmente operáveis mesmo que aconteça alguma falha. Para este sistema é fundamental a criação de uma conta de utilizador de forma a aceder aos sistemas, no entanto permitindo apenas o necessário

[214] (Pinho, 2017)
[215] Art. 32º do RGPD

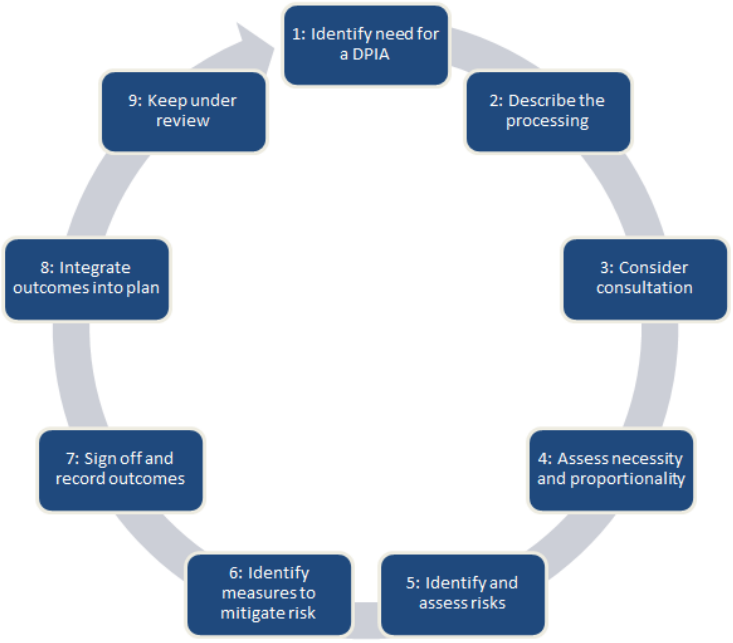
para desempenhar as suas funções. Posteriormente, é necessária a criação de um mapa de acessos com todas as permissões dos colaboradores [216].

4.2.1.2.5 – Avaliação de Impacto sobre a Proteção de Dados

No caso de um determinado tratamento, que, por sua vez, implique um elevado risco para os Titulares de Dados, o responsável pelo tratamento deverá proceder à realização de uma avaliação de impacto antes de iniciar o tratamento. Durante o processo, deverá ser solicitado um parecer ao EPD e um pedido de consulta prévia à Autoridade de Controlo, que será posteriormente abordada.

A avaliação de impacto é um mecanismo que permite à entidade analisar o processo de tratamento e minimizar os potenciais riscos associados à proteção de dados. Apesar de ser um requisito legal quando é apresentado um elevado risco, a avaliação de impacto é um processo contínuo e incorporado nos processos organizacionais da entidade de forma a que os resultados tenham influência na sua estratégia de negócio [217].

Figura 11 - Processo de Avaliação de Impacto sobre a Proteção de Dados



Fonte: (Information Comissioner's Office, 2018)

4.2.1.2.6 – Outros Impactos

Ao destacar o tema da privacidade junto da sociedade e das empresas, o RGPD trouxe também consigo diferenças, não só no online mas também no físico, o que, por sua vez, é também importante para o retalho se este estiver presente no canal físico. Apesar da proteção online ser importante, a proteção de dados guardados em equipamentos antigos ou registados em papel são de igual importância, visto que poderão comprometer o Titular similarmente. Nesse sentido, o RGPD levou os retalhistas que detêm presença em canal físico a consideram medidas

[216] (Portal do DPO, 2018)
[217] (Information Comissioner's Office, 2018)

de segurança física, como os consumidores são supervisonados dentro das instalações, como a entidade dispõe de material eletrónico ou como as instalações são protegidas [218].

4.2.1.3 - Processo de Controlo e Monitorização

De forma a respeitar todos os direitos consagrados pelo regulamento, as empresas têm de ser capazes de remover os dados e/ou garantir acesso aos dados pessoais de um cliente através de todos os canais e sistemas nos quais estão posicionados, assim como tornou obrigatória a verificação explícita e positiva do consentimento e, consequente, revogação por parte dos titulares de dados, assim como a garantia de outros direitos igualmente consagrados no regulamento europeu.

Dessa forma, isto implicou mudanças dentro das empresas, consequentemente, levando-as a adotar mecanismos para assegurar os direitos recentemente consagrados pelo regulamento europeu.

4.2.1.3.1 - Portabilidade dos Dados

Tal como explicado anteriormente[219], a portabilidade de dados resume-se na capacidade de mover e transferir dados entre diferentes aplicações ou programas. Por exemplo, para consumidores, a portabilidade dos dados permite coordenar melhor que tipo de dados têm nas redes sociais. Ao poderem partilhar os dados através de várias plataformas, os utilizadores sabem que a informação está atualizada e não têm que modificá-la em cada *website*. Por sua vez, o RGPD veio solicitar às entidades que incorporem esta possibilidade nas suas plataformas, destacando-a enquanto direito do utilizador [220].

Embora existam barreiras a este tipo de serviço, visto que muitas plataformas têm formatos ou *templates* de dados específicos, a utilização de um formato comum e aberto para armazenar e transferir dados torna a portabilidade dos dados mais simples e fácil. Estes formatos incluem, por exemplo:

- JSON (*Javascript Object Notation*)

O formato JSON destaca-se pela sua capacidade de representar estruturas de dados mais complexas. Baseado na linguagem de programação JavaScript, é legível tanto para humanos como para máquinas. Muitos *websites* utilizam este formato para realizar o intercâmbio de dados entre programas e sistemas [221].

- XML (*Extensible Markup Language*)

O formato XML baseia-se num padrão simples de representar dados estruturados, que tem a particularidade de ser tanto legível para humanos como para máquinas. Embora seja principalmente utilizada para documentos, pode representar estruturas de dados assim como os que são empregues em serviços web. Neste sentido, ficheiros em formato XML podem ser processados por interfaces de programação de aplicações, o que, por sua vez, facilita a troca de

[218] (Information Comissioner's Office, 2018)
[219] Ver subcapítulo 3.2.3.5
[220] (Information Comissioner's Office, 2018)
[221] (Information Comissioner's Office, 2018)

dados. Neste contexto, é facilitada a transmissão de dados para outra entidade, se o Titular de Dados der permissão[222].

- CSV (*Comma-Separated Values*)

Este formato é definido como um formato-padrão que entrega os dados numa folha de cálculo. Os dados são reproduzidos num simples ficheiro de texto, em que cada linha contém dados separados por vírgulas. Este formato é principalmente utilizado para trocar dados e depende de aplicações de software para que funcione. Embora não esteja propriamente normalizado, o facto de ser um formato fácil de operar, estruturado e legível para máquinas, torna-se num formato adequado aquando a resposta a um pedido de portabilidade de dados[223].

- RDF (*Resource Description Framework*)

O formato RDF é uma plataforma que permite a codificação, troca e reutilização de dados estruturados, utilizando um formato XML de base. Desta forma, estrutura os dados e ajuda na interoperabilidade e processamento dos mesmos [224].

4.2.1.3.2 - Esquecimento e Apagamento

Também conhecido como o "direito a ser esquecido", permite aos Titulares submeter um pedido, verbal ou escrito, à entidade que detém os seus dados pessoais para que estes sejam apagados. Este pedido apenas aplica-se segundo as circunstâncias consagradas no art. 17º do RGPD.

Se alguma destas condições for preenchida e o pedido for válido, a entidade deve proceder ao apagamento desses mesmos dados, independentemente do sistema. No caso da informação se tiver tornado pública, a entidade deverá comunicar aos controladores para apagarem de igual modo os dados referentes ao Titular. No entanto, o regulamento europeu não estipula o formato de um pedido válido e define que este pode ser feito a qualquer parte da entidade. Nesse sentido, as entidades, além de se equiparem com mecanismos que sejam capazes de realizar esta tarefa, também tiveram de se preparar para receber pedidos independentemente do canal. Adicionalmente, a entidade teve de elaborar uma política e sistemas que possam registar pedidos que sejam feitos verbalmente [225].

4.2.1.3.3 - Acesso

Aquando a necessidade de solicitar acesso à sua informação, o Titular dos Dados deverá submeter um pedido à entidade. O pedido poderá assumir uma forma verbal ou escrita e é válido se explicitar que o Titular está a pedir acesso aos seus dados pessoais. Aquando a entrega da cópia dos seus dados pessoais, deverá se decidir o formato de entrega, considerando as circunstâncias do pedido e se o Titular dispõe da capacidade para aceder aos dados através desse formato. Dessa forma, é necessário estabelecer opções para os mais variados consumidores e abordar os consumidores sobre qual seria o seu formato pretendido. Por

[222] (Information Comissioner's Office, 2018)
[223] (Information Comissioner's Office, 2018)
[224] (Miller, 1998)
[225] (Information Comissioner's Office, 2017)

exemplo, se o Titular realizar o pedido via eletrónica, a entidade deverá fornecer os dados num formato eletrónico comum, exceto se o Titular solicitar outro formato [226].

4.2.1.3.4 - Retificação

De forma a retificar a informação que uma entidade dispõe acerca de si, o Titular de Dados deverá solicitar um pedido à entidade em questão. Por sua vez, aquando a receção do pedido, a entidade deverá proceder à verificação se os dados em questão são exatos e se é necessário proceder à sua retificação, tendo em consideração os argumentos e as provas levantadas pelo Titular dos Dados.

Apesar disto, existem situações em que definir a exatidão de algum dado é mais complexa. Por exemplo, no caso do erro em si estar correto e deve ser mantido assim. Ou no caso dos dados registarem uma opinião, dada a natureza subjetiva da mesma. Nessa eventualidade, os dados são atualizados com informação adicional atualizada ou são expressamente identificados como uma opinião. Não obstante, enquanto a entidade verifica a exatidão dos dados em questão, a mesma não poderá proceder ao seu tratamento se o Titular assim o desejar [227].

4.2.1.3.5 - Oposição

Tal como explicado anteriormente, o direito de oposição permite ao Titular de Dados opor-se ao tratamento dos seus dados pessoais a qualquer momento. Para isto, o Titular dos Dados deverá solicitar um pedido à entidade relativamente ao tratamento de todos os dados que esta contém sobre o indivíduo ou apenas acerca de algumas informações. Se os dados forem tratados para fins de marketing, este direito é absoluto, logo, não existem isenções ou motivos para a entidade recusar [228].

4.2.1.4 – Processo de Comunicação

O processo de comunicação estipula-se pelo contacto entre a entidade, na qualidade de responsável pelo tratamento, com outras entidades, sejam estas subcontratantes ou uma autoridade de controlo ou até mesmo um Titular de Dados. Tendo isto em consideração, o processo de comunicação difere consoante qual for o recetor.

4.2.1.4.1 - Com o Titular de Dados

Tal como verificamos anteriormente, o RGPD introduziu diferenças substanciais na relação entre o Titular dos Dados e as entidades que os processam ou as que os controlam. No processo de comunicação, estes impactos podem ser divididos em 2 diferentes momentos. O primeiro quando o titular pretende exercer os seus direitos, tal como vimos nas etapas anteriores. O segundo refere-se ao momento em que a entidade estabelece o contacto com o Titular dos Dados.

O segundo momento exerce-se aquando, por exemplo, existe uma violação de dados pessoais. Se tal se suceder e se este evento tiver consequências para "direitos e liberdades das pessoas singulares", a entidade deverá comunicar o evento ao Titular dos Dados, de uma forma simples, clara e com uma breve descrição do sucedido com as informações consagradas no art.º 33º do

[226] (Information Comissioner's Office, 2020)
[227] (Information Comissioner's Office, 2018)
[228] (Information Comissioner's Office, 2018)

RGPD. No entanto, esta comunicação não lhe é exigida se forem preenchidos os requisitos do art.º 34º do mesmo regulamento.

Exemplificando, o roubo de uma base de dados de clientes, que poderá ser utilizada para cometer fraude de identidade, precisaria de ser comunicada aos Titulares de Dados dadas as suas potenciais consequências. No entanto, se forem tomadas medidas para minimizar o risco por parte da entidade, então essa comunicação não é exigida.

Não obstante, esta diferença na comunicação com os Titulares de Dados impacta os processos da entidade. Em primeiro lugar, esta tem de estipular um plano de resposta, caso o evento aconteça. Em segundo lugar, terá de estipular um processo para a avaliação dos potenciais riscos, assim como uma estratégia de comunicação com as partes interessadas [229].

4.2.1.4.2 - Com um subcontratante

Assim como o regulamento impactou a relação entre a entidade e o consumidor, também este influenciou as relações entre entidades. Aquando a necessidade de incorporar um subcontratante no tratamento dos dados, o RGPD estipula que deve existir um contrato entre as duas entidades. Se o subcontratante necessitar de outra entidade para a operação, o responsável pelos dados terá de autorizar, em primeiro lugar, e, posteriormente, também deverá proceder à realização de um contrato com essa entidade [230].

Este ato normativo permite a todas as partes interessadas compreender quais são as suas responsabilidades e as suas obrigações. Da mesma forma, permitem estar em conformidade com o regulamento [231].

Além da realização do contrato, o responsável pelo tratamento está encarregue de efetuar as auditorias e as inspeções necessárias, sendo que se os processos de tratamento não estiverem de acordo com o RGPD, o responsável pelos dados poderá ter de proceder ao pagamento de danos em processos judiciais, sanções ou mesmo medidas corretivas. Posteriormente, se as ações do subcontrante não forem ao encontro do esperado pelo regulamento, também estes poderão ter de enfrentar processos judiciais, multas, sanções ou medidas corretivas [232].

Por sua vez, isto traduz-se na utilização de recursos tanto monetários como humanos, assim como em potenciais punições, caso o tratamento não vá de acordo com o estipulado pelo RGPD. Por outro lado, a apresentação dos contratos apresenta uma determinada salvaguarda para as entidades, caso os seus subcontratantes falhem nas suas obrigações.

4.2.1.4.3 - Com a Autoridade de Controlo

A comunicação com a autoridade de controlo estabelece-se no formato de cooperação, para que esta possa proceder à realização das suas atribuições, tal como disposto no art. 31º do RGPD. Dentro da organização, caso sejam preenchidas algum dos critérios dispostos no art. 37º, o regulamento prevê a necessidade de um Encarregado de Proteção de Dados (EPD). Além

[229] (Information Comissioner's Office, 2018)
[230] Art. 28º nº3 do RGPD
[231] (Information Comissioner's Office, 2018)
[232] Art. 28º nº4 do RGPD

de outras funções, o EPD estabelece a relação de cooperação com a Autoridade de Controlo, ao funcionar como ponto de contacto[233].

Em termos operacionais, o processo de comunicação com a Autoridade de Controlo exerce-se, por exemplo, no caso de uma violação de dados pessoais, onde o responsável pelo tratamento terá de notificar a autoridade de controlo. O mesmo se estabelece entre o subcontratante e o responsável pelo tratamento [234].

No entanto, a entidade não tem de notificar a Autoridade de Controlo se conseguir comprovar que a violação não é suscetível de gerar um risco para o Titular dos Dados. Por exemplo, um retalhista sofre uma violação de dados pessoais quando um colaborador apaga acidentalmente dados de antigos clientes. Estes dados são posteriormente restabelecidos através de uma cópia de segurança. Visto que é improvável que o acontecimento represente um risco para os Titulares de Dados logo não necessitam ser notificados [17].

Não obstante, o responsável pelo tratamento tem de manter um registo de todas as violações de dados pessoais, de forma a que posteriormente, autoridade de controlo possa verificar o cumprimento ou não do regulamento.

Figura 12 - Modelo de registo de tratamento

Ref tratamento	Qual a finalidade	Categorias de Dados tratados				Categorias dos		Fundamento de Licitude
		dados de identificação		dados de contacto		Recursos Humanos	Clientes	
		Dados	prazo de conservação	Dados	prazo de conservação			
TD00	ex: gestão de processamento de salários / gestão de sanções disciplinares / controlo de assiduidade / gestão de clientes / marketing / gravação de chamadas na relação contratual / gestão de processos clínicos / gestão de crédito e solvabilidade	ex: nome, fotografia, número de identificação civil	ex: 10 dias / 2 meses / 3 anos a partir da data da recolha dos dados / 2 anos a partir do fim da relação contratual	ex: morada, e-mail, telefone	ex: 10 dias / 2 meses / 3 anos a partir da data da recolha dos dados / 2 anos a partir do fim da relação contratual	ex: sim	ex: sim	ex: Consentimento, contrato, interesse legítimo, obrigação legal, prestação de serviços de saúd, interesse público ou exercício de autoridade pública

Fonte: (Silva, 2019)

Adicionalmente, aquando a realização de uma avaliação de impacto sobre a proteção de dados que indique que do tratamento decorreria um elevado risco para o Titular dos Dados. Nesse sentido, é necessária uma consulta prévia por parte da Autoridade de Controlo. Se o responsável pelo tratamento não tiver identificado ou minimizado os riscos, a Autoridade de Controlo dá orientações para que do tratamento decorram menores riscos. Este processo pode demorar até 8 semanas a partir da data de receção da consulta, tendo consideração que este prazo pode ser prolongado até mais 6 semanas, atendendo à complexidade do tratamento [235].

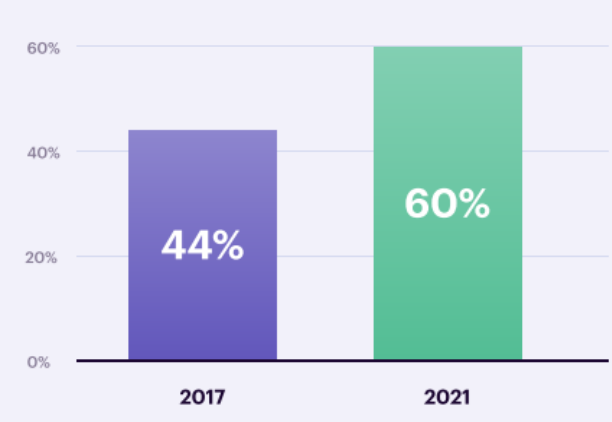
[233] Art. 39º nº1 do RGPD
[234] Art. 33º nº2 do RGPD
[235] Art. 36º do RGPD

4.2.2- Impactos na Experiência do Consumidor

O rápido desenvolvimento tecnológico e *"a proliferação dos canais de venda tornaram os consumidores mais exigentes, complexos e sofisticados"* [236]. Em resposta, os retalhistas começaram a explorar e a apostar mais na área digital de forma a apelarem mais aos seus consumidores e a melhorarem os seus serviços.

A partir deste ponto, a abordagem personalizada tornou-se na resposta essencial para qualquer estratégia de retalho. Um estudo [237] revela que 69% dos consumidores são suscetíveis a comprar marcas que fornecem marketing e comunicação personalizadas. Além disso, o mesmo estudo afirma que 52% dos consumidores admitem que quanto mais a sua experiência de compra for personalizada, maior será a sua satisfação.

Figura 13 - Probabilidade de se tornar um comprador recorrente após uma experiência de compra personalizada (%)



Fonte: (Twilio Segment, 2021)

Como podemos verificar na figura 13, entre 2017 e 2021, a probabilidade de um consumidor regressar à loja depois de uma compra personalizada aumentou cerca 16 pontos percentuais. Desta forma, podemos concluir que *"os consumidores querem que os retalhistas lhes forneçam informação personalizada relevante"* [238]. Esta é transmitida ao consumidor através de recomendações e conteúdos talhados e recorrendo aos canais de comunicação que melhor se adequam a cada consumidor[239].

No entanto, isto apenas é possível graças à possibilidade de os retalhistas recolherem e analisarem dados relativos ao consumidor, para assim também adaptarem o seu conteúdo e as suas ofertas.

Com a integração de todos os canais, é esperado que os retalhistas omnicanal forneçam uma experiência de compra o mais personalizada possível, enquanto respeitam todas as regras implementadas pelo RGPD. Assim, o lema de *"comprar em qualquer altura, em qualquer lugar, em qualquer dispositivo e ao melhor preço"* [240] é acompanhado por um esforço organizacional redobrado face aos jogadores puramente digitais e aos retalhistas tradicionais.

[236] (APDC, 2016)
[237] (Twilio Segment, 2021)
[238] (Lindecrantz, Tjon, & Zerbi, 2020)
[239] (Lindecrantz, Tjon, & Zerbi, 2020)
[240] (APDC, 2016)

A experiência de compra do consumidor no retalho omnicanal recorre a uma série de instrumentos que permitem um maior e melhor contato com os consumidores e uma melhor personalização da experiência de compra, tal como podemos verificar na tabela 2.

Tabela 2 – Exemplos de Tecnologias de Retalho que permitem personalização online e offline

Fase da experiência de compra	**Tecnologia**	**Descrição**	**Objetivo da Personalização**	**Tipo de Dados Recolhidos**
Pré-Compra	*Product Experience Wall*	Um sistema de identificação por radiofrequência interativo que recomenda produtos, consoante o contexto [241]	Recomendações personalizadas Entretenimento Eficiência [51]	Sexo, Idade, Comportamento; Reconhecimento Facial [195]
	Interactive Fitting Room	Sistema de Identificação por radiofrequência que cria um ambiente interativo que conecta o consumidor com o produto, em termos funcionais [242]	Recomendações Personalizadas Apoio à tomada de decisão [51]	Tamanho do corpo do consumidor Informação sobre o produto [196]
	Smart Shelves	Prateleiras digitais que permitem aos retalhistas ter mais controlo sobre o inventário, enquanto possibilitam preços individualizados e comunicação com os consumidores consoante a sua localização [243]	Promoções adaptadas ao consumidor Maior disponibilidade de produtos [51]	Localização dos consumidores na loja
	Digital Kiosk	Tecnologia que dispõe de informação acessível num	Conteúdo Personalizado Combinação entre informação	Conteúdo Digital (Previsões de Tempo, Mapas, entre outros,...)

[241] (Zagel, 2014)
[242] (Moroz, 2019)
[243] (Dekimpe, Geyskens, & Gielens, 2020)

		catálogo físico ou digital, que poderá ser disponibilizado através de ecrãs interativos [244]	e entretenimento [51]	
	Geofencing	Tecnologia que permite que o consumidor seja localizado dentro da loja de forma a enviar ofertas relevantes diretamente para o seu dispositivo (ex. Smartphone) [245]	Recomendações Personalizadas [51]	Dados sobre a localização do consumidor dentro de uma zona virtualmente definida
	Virtual /Augmented Reality	Tecnologia interativa e com informações em tempo real, geradas por um computador (ex. Som, Gráficos, entre outros,…) que permite avaliar o produto em 3D e experimentá-lo ou avaliar como fica com outros acessórios [51] [246]	Visualização do Produto em tempo real Exibição do Produto consoante preferências [51]	Reconhecimento Facial Reconhecimento de Voz
	Service Robots	Dispositivos interativos, estáticos ou móveis, que fornecem mais informações sobre produtos e preços [247]	Recomendações personalizadas, FAQ	Reconhecimento Facial Reconhecimento de Voz Sexo Comportamento
	Voice Command Tech	Dispositivos ativados por comandos de voz e que podem fornecer informações sobre	Informações personalizadas Automatização da experiência de compra [249]	Dados de reconhecimento de voz

[244] (Roggeveen & Sethuraman, 2020)
[245] (Schürmann, 2020)
[246] (Riegger, Klein, Merfeld, & Henkel, 2020)
[247] (Riegger, Klein, Merfeld, & Henkel, 2020)
[249] (Mari, 2019)

		o produto e fazer compras [248]		
	Mobile Apps	Aplicativos instalados no dispositivo móvel do consumidor que permitem a localização dos produtos e/ou que guiam o consumidor até à loja mais próxima [250]	Recomendações personalizadas consoante a localização do consumidor	Dados da localização do consumidor
	Chatbots/Virtual Shopping Assistants	Tecnologia, frequentemente associada a IA, que permite que os retalhistas mantenham uma conexão virtual com o cliente para responder a questões [251]	Respostas Rápidas e Personalizadas Entretenimento	Preferências de Compra Localização Nomes
	Recommendation Agents	Sistema que facilita a tomada de decisão por parte dos clientes em ambientes onde existem uma larga variedade de produtos [252]	Recomendações personalizadas Apoio à tomada de decisão	Histórico de Compras/Pesquisas
	Social Media Listening	Utilização de ferramentas de análise de texto e IA para analisar conversas nas redes sociais e adquirir mais conhecimento sobre o consumidor [253]	Recomendações Personalizadas	Nome Emails Preferências de Compra Localização

[248] (Roggeveen & Sethuraman, 2020)
[250] (Riegger, Klein, Merfeld, & Henkel, 2020)
[251] (Roggeveen & Sethuraman, 2020)
[252] (Moraes, Sanchez, Brown, & Zhang, 2019)
[253] (Roggeveen & Sethuraman, 2020)

	Web-Morphing Personalization	Personalização dinâmica que analisa dados enquanto os consumidores [254]	Recomendações Personalizadas	Preferências e Comportamento do utilizador
Compra	*E-Wallet*	Criação de uma carteira digital que permite débito automático aquando a compra[255]	Facilidade de pagamento	Informações de Transação
	Smart Cart	Tecnologia que permite sondar o carrinho de compras, após o consumidor colocar lá produtos, e, posteriormente, cobrar esse valor numa conta[256]	Facilidade de pagamento	Informações de Transação
	Cloud Computing	Tecnologia que permite aos retalhistas armazenar informações acerca de produtos, registo de compras e inventário, possibilitando o encontro de produtos online mesmo que não estejam na loja física[257]	Facilidade de compra	Informações de Transação
	Drone Delivery	Utilização de *Drones* para a entrega dos Produtos[258]	Facilidade de Entrega	Morada Nome Número de Telemóvel
	Auto-Notification Apps	Notifica automaticamente os consumidores	Facilidade de Entrega e Interação	Nome Número de Telemóvel Interesses Pessoais

[254] (Roggeveen & Sethuraman, 2020)
[255] (Roggeveen & Sethuraman, 2020)
[256] (Roggeveen & Sethuraman, 2020)
[257] (Roggeveen & Sethuraman, 2020)
[258] (Roggeveen & Sethuraman, 2020)

		de disponibilidade de produto[259]		Histórico de Navegação
Pós - Compra	*App-Based Rewards*	Permite que os consumidores tenham acesso a prémios através de transações em determinados canais[260]	Produção de Valor acrescentado para o consumidor com a oferta de incentivos ao consumo	Nome Histórico de Navegação Interesses Pessoais

Estes instrumentos são colocados nos *touchpoints* estabelecidos previamente pelos retalhistas, sejam eles *online* ou *in-store*, e com os quais os consumidores podem ser abordados individualmente. No retalho tradicional, a personalização era feita na loja física e baseava-se na capacidade dos funcionários da loja se adaptarem às preferências dos consumidores[261].

Atualmente, dada a evolução das tecnologias, a personalização baseia-se sobretudo nos dados recolhidos pelos retalhistas, aquando interações (*online* ou *offline*) anteriores com a entidade. Dessa forma, a abordagem de personalização requer uma ampla recolha de dados[262].

A utilização dos dados dos consumidores, por sua vez, representa desafios legais dada a introdução do RGPD no contexto europeu [263]. E, tal como podemos verificar, muitas das tecnologias que ajudam na personalização da experiência de compra também recolhem e tratam Dados Pessoais.

Em termos operacionais, o RGPD exige que, durante a experiência de compra personalizada, o consumidor seja notificado que os seus dados estão a ser recolhidos, seja *online* seja *in-store*. Isto, por sua vez, requer o consentimento e permissão explícita por parte do utilizador para que os seus dados pessoais possam ser tratados, o que adiciona alguns passos extra na conversão do utilizador [264].

Antes do RGPD, este acordo era visto pelas entidades como implícito. Em troca de conteúdo relevante à sua pesquisa, o utilizador fornecia informações sobre o seu comportamento. No entanto, atualmente, o utilizador pode optar por fornecer ou não essa mesma informação, sabendo quais são as finalidades e como vão ser utilizados os seus dados [265].

Por outro lado, em termos organizacionais, os passos adicionais requeridos pelo RGPD permitirão aos retalhistas gerar confiança junto dos utilizadores e consumidores *online* e *in-store*. Ao aplicar os requisitos do RGPD, maior a probabilidade de verem a marca como

[259] (Roggeveen & Sethuraman, 2020)
[260] (Roggeveen & Sethuraman, 2020)
[261] (Riegger, Klein, Merfeld, & Henkel, 2020)
[262] (Riegger, Klein, Merfeld, & Henkel, 2020)
[263] (Nabbosa & Iftikhar, 2019)
[264] Art. 7º do RGPD
[265] Art. 6º do RGPD

confiável, o que, posteriormente, poderá tornar mais fácil a decisão do consentimento por parte do consumidor e/ou utilizador [266] [267].

No caso do retalho omnicanal, de forma a proporcionar uma experiência consistente a cada pessoa, *"independentemente do local que os seus clientes escolham para fazerem compras, os consumidores esperam que a experiência seja a mesma"*. Dessa forma, é necessária uma forma de reconhecer o mesmo consumidor quando interage através de diferentes canais[268]. Isto levanta duas questões, sendo que a primeira se deve à partilha dos dados entre canais e a segunda é relativa à conservação dos dados e definição de perfis.

O primeiro desafio concentra-se na premissa inicial do que é o retalho omnicanal, a partilha de dados entre os vários canais. Dado que na perspetiva do RGPD a entidade é considerada como um todo, esta partilha é permitida entre os diferentes canais. Não obstante, é necessário o consentimento do consumidor/utilizador para realizar este processo, assim como é essencial a utilização de ferramentas de segurança dos dados assegurados por parte do responsável pelo tratamento[269].

O segundo desafio centra-se em definir uma data limite de conservação para estes dados, o qual deve estar alinhado com as finalidades [270]. Por exemplo, um retalhista recolhe dados com a finalidade de personalizar a experiência de compra. De acordo com o RGPD, quando a experiência de compra acabar, os dados deverão deixar de permitir a identificação dos titulares dos dados, pois a finalidade original baseava-se no período da experiência de compra, que entretanto finalizou.

Exemplificando esta questão, nos Países Baixos, algumas empresas de serviços financeiros utilizaram dados transacionais para enviar mensagens de marketing aos titulares desses mesmos dados. A Autoridade de Proteção de Dados Neerlandesa, após a investigação, concluiu que *"se existem dados pessoais a serem recolhidos e processados para executar uma transação, então o tratamento continuado desses mesmos dados pessoais para enviar mensagens de marketing aos titulares é incompatível com a finalidade original do tratamento, em quase todos os casos"*. Desta forma, podemos aferir que os dados não podem ser utilizados para outras finalidades nem ser "reciclados" para uma nova experiência de compra, exceto se isso estiver alinhado com os interesses do titular de dados [271].

Quanto à questão da legalidade de ou não definir um perfil do consumidor. Segundo o RGPD, a definição de perfis é permitida tendo uma base legal. Isto é, em primeiro lugar, o *"consentimento explícito do titular dos dados"* e interesse justificado. Posteriormente, esta definição de perfil, se tiver sido automatizada, deverá ter intervenção humana[272].

4.2.3 - Impactos na Cadeia de Abastecimento

Com o consumidor cada vez mais conectado e com a capacidade de comprar qualquer bem, em qualquer lugar e a qualquer altura, os retalhistas tiveram de se adaptar e remover as barreiras

[266] (DMA (UK) LTD, 2018)
[267] (Cuomo, Genovino, Ceruti, & Tortora, 2019)
[268] (Instituto de Marketing Research, 2019)
[269] Art. 22º nº1 do RGPD
[270] Art. 5º do RGPD
[271] (Ewing, Hickman, & Colin, 2019)
[272] Art. 22º nº3 do RGPD

entre os canais [273]. Isto resultou na criação de estratégias de entrega orientadas para o cliente, como por exemplo:

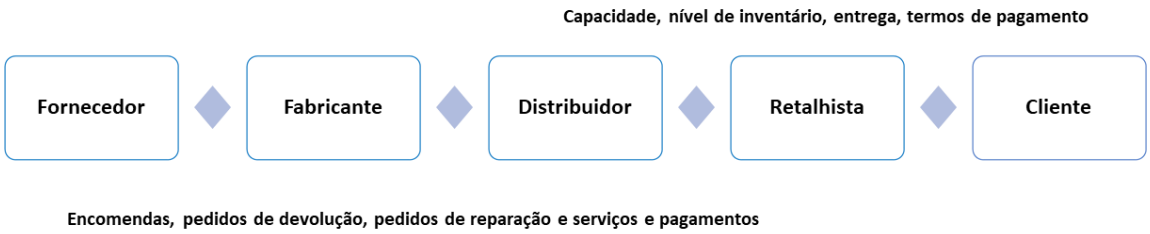
Tabela 3 - Exemplos de estratégias de entrega orientadas para o cliente

Estratégia	**Descrição**
Drop-Shipping	A entidade comercializa produtos que estão no stock do fornecedor
Click and Collect	O cliente compra os bens via online e posteriormente tem a opção de os ir buscar a uma loja física
Reserve and Collect	O cliente reserva online o bem em questão e paga-o numa loja física.
Delivery Lockers	Após a compra, o consumidor recebe um código que, posteriormente, utiliza para adquirir o bem que está num cacifo posicionado em localizações convenientes, como estações de comboio ou supermercados.
Same day delivery	Estratégia de entrega de bens que se foca na loja mais próxima do consumidor e onde a entrega é feita sobretudo em bicicletas ou lambretas

Fonte: (Kuzmicz, 2015)

Estas estratégias são possíveis apenas através da utilização de plataformas integradas entre fabricantes, retalhistas e fornecedores logísticos. Independentemente do canal utilizado, a integração dos dados a partir destas plataformas permitem consultar e partilhar dados exatos e em tempo real [274]. Dessa forma, todas as áreas do negócio estão integradas e a informação é visível entre as diferentes partes interessadas, através de um modelo de *data sharing* [275]. Porém, se esta informação conter dados pessoais, então este fluxo está sob a jurisdição do RGPD.

Figura 14 – Exemplo de Cadeia de Abastecimento



Fonte: (Laudon & Laudon, 2012)

Tendo em consideração a figura 14 e atendendo que o regulamento europeu se destina à proteção dos dados de pessoas singulares, podemos afirmar que, dentro da cadeia de abastecimento, a informação pessoal pode vir de 2 principais fontes: Colaboradores/Fornecedores e Consumidores [276]. Neste contexto, o termo colaborador traduz-se em "*pessoas com um contrato de emprego reconhecido como tal, ao abrigo da legislação*

[273] (Piotrowicz & Cuthbertson, 2014)
[274] (McKenna, 2021)
[275] (Mouton, 2019)
[276] (Pinho, 2017)

laboral aplicável" [277]. Dessa forma, consideram-se colaboradores todos os que se encontram sob responsável pelo tratamento, incluindo fabricantes, fornecedores, retalhistas e distribuidores.

4.2.3.1 RGPD e os dados consumidores em contexto de Cadeia de Abastecimento

Os dados dos consumidores são essenciais para a cadeia de abastecimento, visto que o omnicanal se trata de uma abordagem mais centrada nos mesmos. Tal como estipulamos anteriormente, estes dados permitem extrapolar padrões de consumo, interesses, entre outros, assim como moldam não só aspetos de marketing como também da produção. Isto é apenas possível graças ao modelo de *data sharing* que flexibiliza toda a operação [278].

No entanto, isto pode provocar algumas preocupações com a privacidade, sobretudo relativamente aos consumidores. Por exemplo, uma entidade partilha dados pessoais com outras entidades para realizar um serviço, no entanto sem um consentimento informado do Titular ou Titulares de Dados. Sendo esta situação um acesso não autorizado, torna-se incompatível com os direitos consagrados no RGPD, especialmente o de consentimento.

Para evitar estas situações e, consequentemente, multas para as entidades, à semelhança dos contratos celebrados com os subcontratantes, surgiram os acordos de *Data Sharing* enquanto boas práticas para assegurar a concordância com o regulamento [279]. Além do subcontrante, esta partilha de dados pode acontecer entre também entre Responsáveis.

Exemplificando, a Universidade de Cambridge, nas suas políticas de privacidade, pondera 3 diferentes categorias de *Data Sharing:* (a) entre Responsáveis pelo Tratamento conjuntos para fins conjuntos, (b) com um terceiro para a sua própria utilização e (c) com um subcontratante que guarda e processa os dados recolhidos pela entidade [280]. Dada a natureza da cadeia de abastecimento omnicanal, analisaremos mais em detalhe a troca de dados pessoais entre responsáveis conjuntos.

Esta partilha de dados para fins conjuntos pode ocorrer quando um retalhista partilha dados pessoais (ex. nome, morada, …) com um distribuidor para a entrega do produto ou quando esse retalhista partilha os dados pessoais com um produtor de forma a personalizar o bem. Aquando desta a partilha de dados com um responsável conjunto, as entidades, por motivos legais, em primeiro lugar, estabelecem um acordo de controlo mútuo que define responsabilidades relativamente à proteção de dados. Assim como também partilham esta informação com o Titular dos Dados, por exemplo, através das suas políticas de privacidade [281].

4.2.3.2 RGPD e os dados dos colaboradores em contexto de Cadeia de Abastecimento

A rápida adoção de novas tecnologias de comunicação e informação, por parte das entidades, no local de trabalho, apesar de fomentar a melhoria dos seus processos, também abre espaço para potenciais tratamentos de dados invasivos, os quais podem incluir, por exemplo, a

[277] (Data Protection Working Party, 2017)
[278] (Mouton, 2019)
[279] (Information Comissioner's Office, 2021)
[280] (University of Cambridge, 2018)
[281] (University of Cambridge, 2018)

utilização de serviços online e/ou dados de localização de um dispositivo tecnológico, a partilha de dados de colaboradores com outras partes (*data sharing*) ou até mesmo a monitorização do indivíduo. Tendo isto em conta, estas novas tecnologias podem significar barreiras para a proteção de dados no contexto laboral, sobretudo na cadeia de abastecimento[282].

A cadeia de abastecimento omnicanal é reconhecida pelo seu nível de coordenação e integração entre as partes interessadas (fornecedores, fabricantes, retalhistas e operadores logísticos), assim como também pela troca dinâmica de elevados volumes de dados. Tendo isto em conta, existe uma maior possibilidade da partilha de dados pessoais de uma determinada parte a um nível mais amplo do que aquele que seria necessário, podendo até ser compartilhados ao longo de toda a cadeia. Ultimamente, esta partilha pode resultar em danos e prejuízos para as pessoas singulares e coletivas em questão.

A questão do consentimento é central no RGPD. No entanto, tendo em conta a natureza de uma relação colaborador-entidade, este consentimento raramente é dado de forma livre ou não condicionada, o que, por sua vez, contraria o estabelecido pelo art.º 4º do RGPD. Ou seja, o consentimento acaba por ser insuficiente perante os direitos e liberdades do colaborador [283].

Tendo isto em conta, a entidade pode invocar um interesse legítimo para realizar o tratamento dos dados dos colaboradores. Contudo, este processo implica um teste de proporcionalidade, ou seja, um método que atesta pela necessidade dos dados, se esse tratamento ultrapassa os direitos do Titular dos Dados e avalia as medidas que devem ser tomadas de forma a assegurar a vida privada e o sigilo das comunicações [284]. Desta forma, o tratamento dos dados no contexto laboral, quando legítimo, deverá ser realizado da forma menos intrusiva possível, assim como também deve ser orientada para a área de risco específica [285].

Além disso, visto que qualquer operação de tratamento de dados pessoais deve ir ao encontro do princípio de transparência, anteriormente explicado, ou seja, mesmo sendo colaborador de uma entidade, o indivíduo, na qualidade de Titular de Dados, deverá estar totalmente informado acerca do processo. Assim como deve proceder à realização de uma Avaliação de Impacto, dado a potencial utilização de novas tecnologias para realizar avaliações ou previsões de certos aspetos[286], que remitam para o desempenho do Titular dos dados no trabalho ou até mesmo para os seus dados pessoais[287].

Podemos verificar isto quando um colaborador visita, numa rede social, o perfil de um outro colaborador de forma a recolher dados acerca do mesmo. Embora possa ser argumentado um potencial interesse legítimo em contexto de recrutamento, num cenário em que o colaborador já se encontra em serviço, "*o rastreio das suas redes sociais não deve ter lugar de uma forma generalizada*"[288], devendo apenas ser utilizado na proteção dos seus interesses, privados ou empresariais, e deverá ir de acordo com os princípios estabelecidos pelo RGPD [289].

[282] (Data Protection Working Party, 2017)
[283] (Data Protection Working Party, 2017)
[284] (Ogriseg, 2017)
[285] (Data Protection Working Party, 2017)
[286] (Data Protection Working Party, 2017)
[287] (Ogriseg, 2017)
[288] (Data Protection Working Party, 2017)
[289] (Ogriseg, 2017)

Outro exemplo materializa-se no controlo das comunicações eletrónicas em contexto laboral. Com o recente impacto da Covid-19 e o consequente trabalho remoto, resulta numa monitorização tecnológica fora do contexto laboral e já no interior da esfera privada do colaborador [290]. Tendo isto em conta, é necessário distinguir entre estas duas realidades e, portanto, é uma boa prática a utilização de uma VPN, um método que permite a transferência entre o dispositivo utilizado e a rede da entidade. Outros procedimentos incluem a aquisição de dispositivos que oferecem proteções adicionais relativamente a dados e o estabelecimento de políticas de não utilização de dispositivos laborais na esfera privada [291].

Em linha com a maior busca pela personalização de um serviço ou produto, missão do retalho omnicanal, os colaboradores de uma entidade podem ver os seus dados pessoais a serem partilhados com terceiros, de forma a assegurar este objetivo. Nesse caso, segundo o RGPD, se houver uma troca de informação para além do necessário, a entidade não possui bases legais para as fornecer a terceiros (ex. consumidores).

Os dados pessoais nestes casos podem também assumir a forma de dados referentes ao tempo e presença de um determinado colaborador, à sua geolocalização ou estar, até mesmo, em formato audiovisual [292]. Desta forma, o RGPD veio, por sua vez, regular a forma como as entidades recolhem, tratam e transferem este tipo de dados.

Exemplificando, no que diz respeito, a dados referentes ao tempo e presença de um colaborador, a utilização de sistemas que permitem controlar quem entra em determinadas instalações é legítima, segundo o regulamento, tendo em conta a finalidade de controlar acessos. No entanto, a utilização deste sistema de forma a controlar as atividades dos colaboradores ou avaliar a sua performance não entra em concordância com o RGPD, visto que não coincide com a finalidade inicial [293].

Outro exemplo foca-se nos dados de geolocalização e nos sistemas que os fornecem. Tecnologias que permitem o rastreio e monitorização de veículos têm sido largamente adotados, em especial por parte de entidades que envolvem atividades de transporte ou distribuição. Novamente, isto está em concordância com o RGPD dado o interesse legítimo de localizar o veículo em questão, tanto para a empresa como para o consumidor aquando da entrega de um produto. Não obstante, a rápida evolução destes sistemas permite, além do rastreio, também recolher dados acerca do comportamento ao volante [294].

Consequentemente, o RGPD estipula algumas exigências quanto a este tipo de tratamento como uma avaliação de necessidade, assim como o colaborador deverá estar ciente que o seu comportamento está a ser monitorizado. Se, porventura, o veículo poder ser utilizado para uso privado, a entidade não poderá tratar esses dados e será apropriado a integração de um sistema de *opt-out* (o colaborador tem a opção de desligar temporariamente o rastreio quando circunstâncias especiais justificam essa ação). No entanto, se se comprovar essa necessidade, a implementação deverá ser proporcional aos riscos [295].

[290] (Ogriseg, 2017)
[291] (Data Protection Working Party, 2017)
[292] (Data Protection Working Party, 2017)
[293] (Data Protection Working Party, 2017)
[294] (Data Protection Working Party, 2017)
[295] (Data Protection Working Party, 2017)

4.3 - O Caso Português

Aquando da aprovação do RGPD em 2016, as empresas portuguesas percecionaram o RGPD como uma evolução da anterior diretiva europeia, a 95/46 CE, que também regulava o tratamento de dados pessoais e à livre circulação dos mesmos.

Dessa forma, gerou-se uma necessidade de rever *"todos os fluxos internos de recolha e tratamento de dados"*[296], afirma a empresa A, para *"assegurar que todos departamentos e estrutura poderiam continuar a operar sem qualquer tipo de limitação ou constrangimento dentro do novo quadro legal"*[297]. Sobretudo, porque tal como a Empresa C alega, o tratamento dos dados, previamente ao RGPD, *"começava a ser um caos"*[298].

Segundo as empresas entrevistadas[299], anteriormente à implementação do RGPD, a área da proteção de dados era *"pouco supervisionada/regulada do ponto de vista legal"*[300] e a implementação do regulamento europeu *"foi totalmente necessária"*[301].

De forma a preparar-se para a implementação do regulamento, algumas empresas relataram respostas diferentes. A empresa A, dado o seu regime de subcontratação, alocou uma equipa legal, enquanto consultora, de forma a realizar a transição para o novo enquadramento legal. No caso da empresa B, a primeira ação consistiu na nomeação de um Encarregado de Proteção de Dados, tal como previsto pelo próprio regulamento, e junto dos subcontratantes, celebraram-se acordos de tratamento de dados. Por outro lado, a empresa C apenas começou *"a trabalhar na implementação meses antes da data"* [302] e estabeleceu como prioridade a digitalização.

Nesse sentido, *"eliminar o papel e tornar a empresa (...) mais digital*" [303] foi um dos principais impactos criados pelo RGPD, segundo a empresa C. Pois, até à data, o registo era feito com uma ficha de papel e, à luz do novo regulamento, se o cliente ou uma autoridade de controlo exigisse a prova de que se fez a inscrição, seriam *"eram caixas e caixas e caixas de folhas de papel"* [304], o que dificultaria essa operação. Dessa forma, tal como afirma a empresa A, este regulamento traduziu-se num *"melhor conhecimento e controlo internos"*[305], o que, por sua vez, tornou os processos mais robustos e seguros.

Consequentemente, pode-se concluir que, a nível de processos internos, houve também um impacto significativo dentro as empresas. Tal como podemos concluir anteriormente, o RGPD veio introduzir novos mecanismos de segurança como a questão do consentimento que, para a empresa C, em termos práticos, passou pela incorporação de um processo de assinatura digital. Tal como a empresa B relata, também se introduziram os registos de atividades de tratamento de dados, as avaliações de impacto sobre a proteção de dados e ainda se alteraram os processos de desenvolvimento, tanto numa vertente de *privacy-by-default* como também numa perspetiva de *privacy-by-design.* Assim, alteraram-se modelos de atendimento, de forma a ter conta "tanto

[296] Ver página 78 do presente estudo
[297] Ver página 78 do presente estudo
[298] Ver página 79 do presente estudo
[299] Ver anexos
[300] Ver página 78 do presente estudo
[301] Ver página 79 do presente estudo
[302] Ver página 79 do presente estudo
[303] Ver página 80 do presente estudo
[304] Ver página 80 do presente estudo
[305] Ver página 84 do presente estudo

a experiência como a privacidade e segurança da informação do cliente", respeitando o regulamento.

Similarmente, o RGPD levou a uma revisão das políticas de segurança informática por parte das empresas. Contudo, houve a necessidade de criar várias ferramentas internas, sobretudo na área de gestão de acessos, isto é, *"definir quem é que efetivamente precisava de aceder à informação dos clientes"*[306], assim como na área de retenção de dados pois, tal como defende a empresa C, o RGPD introduziu *"datas de validade"*[307] para os dados pessoais. Isto, por sua vez, criou a necessidade de ações de formação, consoante as especificidades de cada canal, relata a empresa B. Mesmo a empresa C, também relata a carga legal dada a necessidade de "*conhecer e analisar (...) o que está na legislação*"[308].

Como resultado, todas estas implementações e mudanças implicaram custos associados, cargas administrativas maiores e "dores de crescimento", afirmam todos os entrevistados. No entanto, na visão da empresa C, todo este investimento, embora necessário, não se pode traduzir num retorno financeiro, porque *"não é percebido pelo cliente"*[309] e a *"perceção do consumidor (...) é reduzidíssima"*[310].

Não obstante, a crescente opinião pública acerca da proteção de dados também impulsionou a implementação do RGPD, o que, por sua vez, tornou o mercado mais confiável, segundo a empresa C. Dessa forma, ao apostar na questão da privacidade, para a empresa B, existe também um maior investimento ao nível da satisfação do cliente. Tendo isto em conta, a empresa A concluiu que o RGPD funcionou com um "*ponto de referência*"[311].

Tabela 4 - Impactos Positivos e Negativos registados pelas empresas portugueses

Impactos Positivos	**Impactos Negativos**
- Digitalização - Alterações nos processos internos - Favorável Opinião Pública	- Burocracia/Carga Administrativa - Custos de Implementação

Embora os impactos negativos incluam questões como a burocracia e os custos de implementação, os entrevistados registam que não existe nenhum efeito negativo a longo prazo ou continuados. Contudo, os entrevistados acreditam que existem algumas falhas que podem ser trabalhadas pelo RGPD. Alguns destes aspetos incluem as coimas "*que se afiguram muito avultadas*"[312] ou que a regulação de forma não "*muito exata*"[313] relativamente "*à presença e à identificação online*"[314], sobretudo na área de rastreio e publicidade, como afirma a empresa C.

[306] Ver página 80 do presente estudo
[307] Ver página 81 do presente estudo
[308] Ver página 81 do presente estudo
[309] Ver página 82 do presente estudo
[310] Ver página 81 do presente estudo
[311] Ver página 85 do presente estudo
[312] Ver página 87 do presente estudo
[313] Ver página 85 do presente estudo
[314] Ver página 85 do presente estudo

Conclusão

Os avanços tecnológicos dos últimos anos deram lugar a disrupções em todos os setores de atividade. No setor do retalho, uma destas inovações levou a um aumento exponencial dos canais de venda, originando assim a estratégia. Posteriormente, com a mudança dos hábitos de consumo e com o objetivo de melhorar a experiência do cliente, esta evoluiu para uma estratégia omnicanal.

O retalho omnicanal inclui a integração de todos os canais de venda para fornecer ao consumidor uma experiência de compra sem barreiras e ao retalhista um ponto de vista unificado sobre quem é o consumidor. Neste sentido, a proteção de dados, nomeadamente o RGPD, provocou alguns impactos neste modelo de gestão de canais, de forma a proteger os dados pessoais dos consumidores europeus.

Tendo em vista este estudo, conclui-se que os principais impactos criados pelo RGPD foram, sobretudo, operacionais, isto é, criaram alterações nos processos internos das empresas. Na tabela seguinte, verificam-se os impactos de uma forma breve e concisa.

Tabela 5 – Principais impactos do RGPD no Retalho Omnicanal

Áreas-Chave	**Principais impactos**
Recolha e Tratamento de Dados	O RGPD alterou significativamente o processo de recolha e tratamento de dados. Por sua vez, este incorporou datas para o tratamento dos dados e introduziu o conceito de consentimento e vários outros direitos que, consequentemente, levaram a uma monitorização dos mesmos e ainda à comunicação no caso da sua violação;
Personalização	Dada a necessidade de dados pessoais para estabelecer uma relação personalizada, o RGPD impacta este processo ao determinar direitos e deveres das empresas
Cadeia de Abastecimento	Com a integração dos canais, a partilha de dados é uma realidade, no entanto, o RGPD impacta a forma como as empresas tratam os dados dos consumidores, colaboradores e parceiros, tudo ao longo da cadeia de abastecimento.
Digitalização	A introdução do RGPD criou oportunidades para a digitalização das empresas que, outrora, tinham os seus processos não-digitalizados, como por exemplo a empresa C;
Burocracia/Investimento	Estas alterações traduziram-se num esforço administrativo e num grande investimento por parte das empresas;

Referências Bibliográficas

Abbott, L. (1955). Quality and Competition: An Essay in Economic Theory. *Columbia University Press*.

Ansari, A., & Mela, C. (maio de 2003). E-Customization. *Journal of Marketing Research, 40*, pp. 131-145.

APDC. (2016). *A Economia Digital em Portugal.* APDC.

Arora, S., & Sahney, S. (2017). Webrooming behaviour: a conceptual framework. *International Journal of Retail & Distribution Management*, 762-781.

Assembleia da República. (2019). Lei n.º 58/2019. 3 - 40.

Associação Nacional dos Industriais de Laticínios. (05 de 06 de 2020). Prevê-se um aumento de 3.6% de compradores online até 2021. Fonte: https://www.anilact.pt/info/actual/mercado/item/5141-preve-se-um-aumento-de-3-6-de-compradores-online-ate-2021

Associação Portuguesa de Empresas de Distribuição. (30 de 03 de 2021). *Vendas no retalha com quebra de 1,5% em ano de pandemia*. Fonte: APED: http://aped.pt/2021/03/30/vendas-no-retalho-com-quebra-de-15-em-ano-de-pandemia/

Barreto, A. (2020). *Direito da Preoteção de Dados à luz do RGPD e da Lei nº58/2019.* Porto: Almedina.

Beck, N., & Rygl, D. (2015). Categorization of multiple channel retailing in Multi-, Cross-, and Omni-Channel Retailing for retailers and retailing. (J. o. Services, Ed.) pp. 171-175.

Belcic, I. (25 de agosto de 2021). *A Complete Guide to Web Tracking (and How to Avoid It)*. Fonte: avast: https://www.avast.com/c-web-tracking?v=rb

Besemer, L. (14 de dezembro de 2018). *Digital Marketing - The impact of GDPR*. Fonte: EXIN: https://www.exin.com/data-protection/digital-marketing-impact-gdpr/

Brakus, J. J., Schmitt, B., & Zarantonello, L. (maio de 2009). Brand Experience: What Is It? How Is It Measured? Does It Affect Loyalty? *Journal of Marketing, 73*, pp. 52-68.

Chan, J. (2013). *The Promise of Digital Technology in Brick and Mortar Retail.* Massachusetts: Massachusetts Institute of Technology.

Chaturvedi, N., Martich, M., Ruwadi, B., & Ulker, N. (2013). *The future of retail supply chains.*

Chellappa, R., & Sin, R. (abril de 2005). Personalization versus privacy: An Empirical Examination of the Online Consumer's Dilemma. *Information Technology and Management, 6*, pp. 181-202.

Chivot, E., & Castro, D. (2019). *The EU Needs to Reform the GDPR to remain competitive in the Algorithmic Economy.* Center for Data Innovation.

Chopra, S. (2018). The Evolution of Omni-Channel Retailing and its Impact on Supply Chains. *Transportation Research Procedia, 30*, pp. 4-13.

Correia, P., & Jesus, I. (2014). O lugar do conceito de privaciade numa sociedade cada vez mais orwelliana. *Direito, Estado e Sociedade*, pp. 135-161.

Cramer-Flood, E. (2021). *Global Ecommerce Update 2021*. eMarketer. Fonte: https://www.emarketer.com/content/global-ecommerce-update-2021

CrowdFlower. (2017). *Data Scientist Report.* CrowdFlower.

Cunha, L. (outubro de 2015). A Gestão Omnicanal no Retalho em Portugal: Uma Proposta com Base no Perfil dos Consumidores.

Cuomo, M., Genovino, C., Ceruti, F., & Tortora, D. (Dezembro de 2019). The impact of GDPR on brand's responsability. *Contemporary Issues in Branding* , pp. 58-71.

Dalsey Hillblom Lynn. (22 de setembro de 2020). *Omnichannel Logistics*. Fonte: DHL: https://www.dhl.com/global-en/home/insights-and-innovation/thought-leadership/trend-reports/omni-channel-logistics.html

Danon, S. (2017). *GDP Top Ten #6: Privacy by Design and by Default*. Fonte: Deloitte: https://www2.deloitte.com/ch/en/pages/risk/articles/gdpr-privacy-by-design-and-by-default.html

Data Protection Working Party. (8 de junho de 2017). Opinion 2/2017 on data processing at work. Bruxelas.

Dekimpe, M., Geyskens, I., & Gielens, K. (2020). Using technology to bring online convenience to offline shopping. *Marketing Letters, 31*, pp. 25-29.

Deloitte. (2021). *Global Powers of Retailing.* Deloitte.

Deloitte China. (2020). *"Future Consumer" Series: Omnichannel Transformation Begins by Grasping the Key to Consumer Mentalities.* Deloitte.

Demétrio, D. (dezembro de 2003). Infra-Estrutura de Protocolação Digital de Documentos. Florianópolis, Brasil.

Dennis, C., Alamanos, E., Papagiannidis, S., & and Bourkakis, M. (2014). *Does social exclusion influence multiple channel use? The interconnections with community, happiness and well-being.* Journal of Business Research. Elsevier.

DMA (UK) LTD. (2018). *GDPR: A consumer Perspective.*

DMN News. (25 de maio de 2018). *Cookies and Consent: How GDPR Impacts Online Tracking*. Fonte: DMN News: https://www.dmnews.com/retail/article/13034543/cookies-and-consent-how-gdpr-impacts-online-tracking

Ecommerce Europe. (2019). *European Ecommerce Report.* Ecommerce Europe.

ecommerceDB. (13 de 12 de 2019). *The eCommerce market in Portugal*. Fonte: ecommerceDB: https://ecommercedb.com/en/markets/pt/all

eMarketer. (2020). *Retail Ecommerce Sales in China, 2019-2024.* eMarketer.

eMarketer. (2020). Top 10 Countries Ranked by Retail Ecommerce Sales Share 2021 & 2022. *eMarketer*.

European Comission. (2018). *What does data protection 'by design' and 'by default' mean?* Fonte: European Comission: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_en

European Data Protection Supervisor. (2018). *The History of the General Data Protection Regulation*. Fonte: https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en

Eurostat. (2021). *Volume of retail trade up by 2.7% in euro area and by 2.6% in the EU.* eurostat.

Ewing, C., Hickman, T., & Colin, N. (julho de 2019). Regulator prohibits use of transaction data for marketing purposes. *data, Privacy & Cybersecurity*. White&Case.

Francis, J., & White, L. (2004). Internet Retailing: Back to the Future. *Faculty of Commerce - Papers*, pp. 1-7.

Freund, G., Fagundes, P., Macedo, D., & Dutra, M. (junho de 2019). Mecanismos tecnológicos de segurança da informação no tratamento da veracidade dos dados em ambientes Big Data. *Perspectivas em Ciência da Informação, 24*(2), pp. 124-142.

Geyser, W. (19 de maio de 2021). *GDPR and Social Media: What Data Protection and Privacy Mean for Social Media Marketers*. Fonte: Influencer Marketing Hub: https://influencermarketinghub.com/gdpr-social-media/

Gupta, S., Lehmann, D., & Stuart, J. (2004). Valuing Customers. *Journal of Marketing Research*, 7-18.

Holbrook, M., & Hirschman, E. (1982). The Experimental Aspects of Consumption: COnsumer Fantasies, Feelings, and Fun. *Journal of Consumer Research, 9*(2), 132-140.

ICO. (26 de Maio de 2018). *Data protection by design and default*. Fonte: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/

Information Comissioner's Office. (21 de novmebro de 2017). *Right to erasure*. Fonte: Information Comissioner's Office: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/

Information Comissioner's Office. (11 de dezembro de 2018). *Contracts*. Fonte: Information Comissioner's Office: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/contracts/

Information Comissioner's Office. (20 de dezembro de 2018). *Data protection impact assessments*. Fonte: Information Comissioner's Office: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

Information Comissioner's Office. (24 de janeiro de 2018). *How do we document our processing activities*. Fonte: Information Comissioner's Office: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/documentation/how-do-we-document-our-processing-activities/

Information Comissioner's Office. (10 de janeiro de 2018). *Personal data breaches*. Fonte: Information Comissioner's Office: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

Information Comissioner's Office. (3 de maio de 2018). *Right to data portability*. Fonte: Information Comissioner's Office: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-data-portability/

Information Comissioner's Office. (28 de março de 2018). *Right to retification*. Fonte: Information Comissioner's Office: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-rectification/

Information Comissioner's Office. (7 de abril de 2018). *Security*. Fonte: Information Comissioner's Office: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/

Information Comissioner's Office. (21 de outubro de 2020). *Right to access*. Fonte: Information Comissioner's Office: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/

Information Comissioner's Office. (2021). *Data sharing: a code of practice*. Fonte: Information Comissioner's Office: https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/data-sharing-a-code-of-practice/

Instituto de Marketing Research. (15 de abril de 2019). *Retalho Omnicanal: Para cada canal o mesmo conceito*. Fonte: Instituto de Marketing Research: https://www.imr.pt/pt/noticias/retalho-omnicanal-para-cada-canal-o-mesmo-conceito

Instituto Nacional de Estatística. (2021). *Índices de Volume de Negócios, Emprego, Remunerações e Horas Trabalhadas no Comércio a Retalho.* INE. Acesso em Abril de 2021

Instituto Nacional de Estatística. (2021). *Um ano de pandemia: uma breve síntese.* INE.

iubenda. (maio de 2020). *Cookies and the GDPR: What's Really Required?* Fonte: iubenda: https://www.iubenda.com/en/help/5525-cookies-gdpr-requirements

Jocevskim, M., Arvidsson, N., Miragliotta, G., Ghezzi, A. G., & Mangiaracina, R. (2019). Transitions towards omni-channel retailing strategies: a business model perspective. *International Journal of Retail & Distribution Management*, 3-7.

Kahn, B., Inman, J. J., & Verhoef, P. C. (1 de agosto de 2018). Introduction to Special Issue: Consumer Response to the Evolving Retailing Landscape. *Association for Consumer Research, 3*(3), pp. 255-259.

Kalaignanam, K., Kushwaha, T., & Rajavi, K. (30 de maio de 2018). How Does Web Personalization Create Value for Online Retaiers? Lower Cash Flow Volatility or Enhanced Cash Flows. *Journal of Retailing, 94*, pp. 265-279.

Kuzmicz, K. (19 de outubro de 2015). Benchmarking in Omni-channel Logistics. *Research in Logistics & Production, 5*(5), pp. 491-501.

Laudon, K., & Laudon, J. (2012). Achieving Operational Excellence and Customer Intimacy: Enterprise Applications. Em K. Laudon, & J. Laudon, *Management Information Systems: Managing the Digital Firm* (11ª ed., p. 343). Pearson.

Laudon, K., & Traver, C. (2017). E-commerce - Business. Technology. Society. Em K. Laudon, & C. Traver, *E-commerce - Business. Technology. Society* (13ª ed., pp. 553-655). Pearson.

Li, Z. S., Werner, C., Ernst, N., & Damian, D. (16 de Fevereiro de 2020). GDPR Compliance in the Context of Continuous Integration. *EEE TRANSACTIONS ON SOFTWARE ENGINEERING*.

Lindecrantz, E., Tjon, M., & Zerbi, S. (28 de abril de 2020). *Personalizing the customer experience: Driving differentiation in retail*. Fonte: McKinsey & Company: https://www.mckinsey.com/industries/retail/our-insights/personalizing-the-customer-experience-driving-differentiation-in-retail

Lobato, L., & Zorzo, S. (s.d.). *Avaliação dos mecanismos de Privacidade e Personalização na Web*. Departamento de Computação. São Carlos: Universidade Federal de São Carlos. Fonte: http://www2.dc.ufscar.br/~zorzo/privperson/pdf/clei2006_Lobato_Zorzo.pdf

Machado, D., & Doneda, D. (dezembro de 2018). Proteção de dados pessoais e criptografia: tecnologias criptográficas entre aninimização e pseudonimização de dados. *Revista dos Tribunais, 998*, pp. 99-128. Fonte: Universidade de Coimbra.

Mari, A. (2019). Voice Commerce: Understanding Shopping-Related Voice Assistantes and their Effect on Brands. *IMMAA Annual COnference.* Doha.

McKenna, N. (Setembro de 2021). *Why is Systems Integration Important?* Fonte: McKenna Consultants: https://www.mckennaconsultants.com/why-is-systems-integration-important/

McKinsey. (2020). *The quickening*. Fonte: Mckinsey Quarterly: https://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/five-fifty-the-quickening

Miller, E. (novembro de 1998). An Introduction to the Resource Description Framework. *Bulletin of the American Society for Information Science*.

Ministério do Comércio e Turismo. (12 de Agosto de 1985). Decreto-Lei nº 339/85. Fonte: https://www.igf.gov.pt/leggeraldocs/DL_339_85.htm

Ministério Público. (14 de 02 de 2014). Decreto-Lei 24/2014. Fonte: http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=2062&tabela=leis&so_miolo=&fbclid=IwAR3L_xiRunzJoQFs0vbnCl0E5o07I6Ol2wAYYU7Qe-jVw0LsmWuH2xHGNzM

Ministério Público. (11 de abril de 2020). Lei nº 65/2020.

Mirsch, T., Lehrer, C., & Jung, R. (junho de 2016). Channel Integration towards Omnichannel Integration. pp. 4-6.

Moraes, H., Sanchez, O., Brown, S., & Zhang, B. (2019). Trust and Distrust in Big Data Recommendation Agents. *Fortieth International Conference on Information Systems*, (pp. 1-15). Munich.

Moroz, M. (2019). Tendency to Use the Virtual Fitting Room in Generation Y - Results of Qaulitative Study. *Foundations of Management, 11*, pp. 239-252.

Mouton, A. (28 de maio de 2019). *Data sharing: what are the prospects for the supply chain?* Fonte: Mobility Work: https://mobility-work.com/blog/data-sharing-supply-chain/

Município de Vila Nova de Famalicão. (18 de Julho de 2012). Regulamento n.º 278/2012.

Nabbosa, V., & Iftikhar, R. (2019). Digital Retail Challenges within the EU: Fulfillment of Holistic Customer Journey Post GDPR. *ICEBT*. Madrid: Association for Computing Machinery.

Nakamura, E., & Geus, P. (2007). *Segurança de redes em ambientes cooperativos.* São Paulo: Novatec.

Neslin, S. A., & Shankar, V. (2009). Key Issues in Multichannel Customer Management: Current Knowledge and Future Directions. *Journal of Interactive Marketing*, 70-81.

Neslin, S., Grewal, D., Leghorn, R., Shankar, V., Teerling, M., Thomas, J., & Verhoef, P. (Novembro de 2006). (J. o. Research, Ed.) *Challenges and Opportunities in Multichannel Customer Management*, p. 96.

Ogriseg, C. (2017). GDPR and Personal Data Protection in the Employment Context. *Labour and Law Issues, 3*(2), pp. 2421-2695.

Pais Mamede, R., Pereira, M., & Simões, A. (2020). *Protugal: Uma análise rápida do impacto da COVID-19 na economia e no mercado de trabalho.* Organização Internacional do Trabalho.

Pajovic, S. (25 de 03 de 2020). 8 Largest eCommerce Companies in the World and No, Alibaba is Not the Largest Chinese eCommerce. Fonte: https://axiomq.com/blog/8-largest-e-commerce-companies-in-the-world/

Pan, Y., & Zinkhan, G. (Abril de 2006). Exploring the impact of online privacy disclosures on consumer trust. *Journal of Retailing*, pp. 331-338.

Parlamento Europeu. (4 de Maio de 2016). Regulamento Geral de Proteção de Dados. pp. 32-88.

Pine, B. J., & Gilmore, J. H. (1998). Welcome to the Experience Economy. *Harvard Business Review.*

Pinho, F. (2017). Anonimização de base de dados de acordo com a Nova Regulamentação Europeia de Proteção de Dados. Porto, Portugal: Universidade do Porto.

Piotrowicz, W., & Cuthbertson, R. (2014). Introduction to the Special Issue Information Technology in Retail: Toward Omnichannel Retailing. *International Journal of Electronic Commerce, 18*(4), pp. 5-16.

Portal do DPO. (16 de junho de 2018). *Requisitos Técnicos de Segurança*. Fonte: Portal do DPO: https://www.portaldodpo.pt/blog/service/requisitos-tecnicos-de-seguranca/

Riegger, A.-S., Klein, J. F., Merfeld, K., & Henkel, S. (outubro de 2020). Technology-enabled personalization in retail stores: Understanding drivers and barriers. *Journal of Business Research, 123*, pp. 140-155.

Rigby, D. (12 de 2011). The future of Shopping. *Harvard Business Review.*

Roggeveen, A., & Sethuraman, R. (março de 2020). Customer-Interfacing Retail Technologies in 2020 & Beyond: An Integrative Framework and Research Directions. *Journal of Retailing, 96*, pp. 299-309.

Rotar, A. (2021). *Europe: retail e-commerce revenue forecast from 2017 to 2025.* Statista.

Ruiz, L. (2018). GDPR in the age of Omnichannel Retail. pp. https://www.retailgazette.co.uk/blog/2018/03/gdpr-age-omnichannel-retail/.

Savills. (2020). *Impact of Covid-19 on European retail.* Savills Research.

Schaverien, A. (2018). Five Reasons Why Amazon Is Moving Into Bricks-And-Mortar Retail. *Forbes*. Fonte: https://www.forbes.com/sites/annaschaverien/2018/12/29/amazon-online-offline-store-retail/?sh=1654f5d25128

Schürmann, K. (11 de março de 2020). *Digitalization of retail: Is the GDPR a brake on innovation?* Fonte: irglobal: https://www.irglobal.com/article/digitalisation-of-reatil-is-the-gdpr-a-brake-on-innovation-38a1/

Sêmola, M. (2014). *Gestão da Segurança da Informação: Uma Visão Executiva.* São Paulo: Elsevier.

Shah, D., Rust, R. T., Parasuraman, A., Staelin, R., & Day, G. S. (2006). The Path to Customer Centricity. *Journal of Service Research*, 103-124.

Shen, A., & Ball, D. (abril de 2009). Is personalization of services always a good thing? Exploring the role of technology-mediated personalization (TMP) in service relationships. *Journal of Services Marketing, 23*(2), pp. 80-92.

Silva, G. (fevereiro de 2019). RDPD aplicado nas PME portuguesas.

Sorescu, A., Frambach, R., Singh, J., Rangswamy, A., & Bridges, C. (2011). Innovations in Retail Business Models. *Journal of Retailing*, S3-S16.

Sunikka, A., & Bragge, J. (2012). Applying text-mining to personalization and customization research literature - Who, what and where? *Expert Systems with Applications, 39*, pp. 10049-10058.

Twilio Segment. (2021). *The State of Personalization 2021*. Twilio Segment.

Unbox Social. (13 de agosto de 2018). *Impact of GDPR on Social Media Marketing - Unbox Social*. Fonte: Medium: https://medium.com/@unboxsocial/impact-of-gdpr-on-social-media-marketing-unbox-social-2f5f6b025db

Universidade de Coimbra. (14 de fevereiro de 2021). *Anonimização e Pseudonimização*. Fonte: Universidade de Coimbra: https://www.uc.pt/protecao-de-dados/protecao_dados_pessoais/anonimizacao

University of Cambridge. (20 de abril de 2018). *Data sharing and using data processors*. Fonte: University of Cambridge: https://www.information-compliance.admin.cam.ac.uk/data-protection/guidance/data-sharing

Verhoef, P., Kannan, P., & Jeffrey, I. (março de 2015). From Multi-Channel Retailing to Omni-Channel Retailing. (J. o. Retailing, Ed.) *Journal of Retailing, 91*, pp. 174-181.

Verhoef, P., Lemon, K., Parasuraman, A., Roggeveen, A., Tsiros, M., & Schlesinger, L. (janeiro de 2009). Costumer Experience Creation: Determinantes, Dynamics and Management Strategies. *Journal of Retailing, 85*, pp. 31-41.

Vilumns, A. (9 de janeiro de 2018). *General Data protection Regulation (GDPR) and subscriber's consent to receive emails*. Fonte: Mailigen by pipedrive: https://www.mailigen.com/blog/gdpr-and-subscribers-consent/

WARC. (22 de 04 de 2013). *eBay aims to be "omnichannel"*. Fonte: WARC: https://www.warc.com/newsandopinion/news/ebay-aims-to-be-omnichannel/31294

Weilland, D. (23 de 12 de 2016). Omnichannel as a New Challenge for Logistics. *Torun Business Review*, pp. 76-77.

Working Party 243. (2017). *Orientações sobre os encarregados da proteção de dados (EPD)*. Comissão Europeia.

Zagel, C. (2014). Product Experience Wall: A Context-adaptive Outfit Recommender System. Em M. Koch, A. Butz, & J. Schlichter, *Mensch und Computer* (pp. 367-370). Oldenburg Wissenschaftsverlag.

Zhang, J., Farris, P., Kushwaha, T., Irvin, J., Steenburgh, T., & Weitz, B. (2010). *Crafting integrated multichannel retailing strategies.* Journal of Interactive Marketing.

Zhang, T., Agarwal, R., & Lucas, H. (dezembro de 2011). The Value of IT-Enabled Retailer Learning: Personalized Product Recommendations and Customer Store Loyalty in Electronic Markets. *MIS Quarterly, 35*(4), pp. 859-881.

Anexos – Transcrições das entrevistas orais e escritas

1. Em primeiro lugar, qual foi a primeira percepção da sua empresa relativamente ao RGPD quando foi lançado em 2016?

(Empresa A) A perceção da empresa após a publicação do RGPD em 2016 foi a de que este novo conjunto de disposições que visava regulamentar uma área de atuação que era, até à data, pouco supervisionada/regulada do ponto de vista legal, iria obrigar à revisão de todos os fluxos internos de recolha e tratamento de dados; não necessariamente culminando na sua alteração ou cancelamento por incumprimento, mas sim numa ótica de assegurar que todos departamentos e estrutura poderiam continuar a operar sem qualquer tipo de limitação ou constrangimento dentro do novo quadro legal.

Houve, naturalmente, a perceção de que este processo de adaptação teria custo e investimento associados, mas contrabalançada com a certeza de que o mesmo processo configuraria uma oportunidade de sistematização de fluxos de informação que, fruto do seu surgimento e crescimento orgânicos, não estavam bem estruturados ou documentados.

(Empresa B) Ora bem, dentro do enquadramento do RGPD também estudou o que esteve na base, a diretiva, a lei 67. O RGPD não apareceu do nada, não é? Já havia uma diretiva europeia, a 95/46/CE que foi transporta para a lei portuguesa, através da lei 67, e, portanto, o RGPD foi um evoluir. Nesse sentido para nós, enquanto empresa, não é que não tenha dado trabalho, mas foi natural. Encaramos com naturalidade até porque já estávamos de alguma maneira à espera.

Porque é que houve necessidade de a Comissão/União Europeia lançar uma legislação? Acho que o Regulamento em si, permite também uma aplicação homogénea em cada estado-membro dos objetivos e princípios de proteção dos dados pessoais que já resultavam da diretiva 95/46/CE e acho que alguns pontos que convém também, para enquadramento, desde já destacar.

Primeiro, a função tecnológica. Portanto, nos últimos anos tem-se assistido a uma evolução tecnológica enorme, grandes saltos no tratamento dos dados e, portanto, achamos que, parece apropriado que tenha havido uma evolução da legislação para acompanhar esta evolução tecnológica, do contexto digital, o eletrónico e consequentemente o tratamento de dados pessoais que lhe está associado. E a própria proteção das pessoas singulares que estão neste contexto.

Depois, também de alguma maneira, acho enquanto no espírito da União Europeia querer criar igualdades de oportunidades e direitos e também a própria homogeneidade dos cidadãos no contexto do tratamento de dados na União Europeia.

Também acho que a livre circulação é outro *driver* que necessitou de ser regulado no que aos dados pessoais diz respeito. Portanto, consequentemente, a União Europeia ao estar a afixar regras para a partilha de informação, sobretudo para aqueles players que estão fora do espaço da União, estamos a falar de gigantes de tratamentos, e que a partir do momento em que essas

entidades fora da União Europeia façam tratamentos dos dados dos cidadãos que estão na União Europeia, sejam regulados do mesmo modo trazendo assim um nivelamento das regras e dos diferentes players no mercado concorrencial. A livre circulação, à semelhança do que aconteceu com os bens, no caso dos dados pessoais, também é a condição fundamental para crescimento e para prosperidade

Depois também a mudança de paradigma no que se refere ao cumprimento controlado. Ou seja, a introdução de um mecanismo de responsabilização das empresas ao invés do espírito anterior que era a autoridade de controlo que fazia essa fiscalização, digamos assim. Portanto, houve uma responsabilização das empresas nesse sentido e também seriam responsáveis pela evidenciação do cumprimento das mesmas. E, portanto, nesse sentido facilita-se o papel da própria autoridade de controlo, que continua com a mesma responsabilidade de reforçar o cumprimento e de ver se o cumprimento está a ocorrer.

E acho que talvez, apesar de ser a última que falo, é das mais importantes é a proteção do Estado Europeu, no sentido de a proteção das atividades económicas ao nível da União, prevenindo a distorção da concorrência, até porque ao nível do digital e os dados (Big Data) são um caminho necessário e fundamental para a prosperidade, para o crescimento e para se manter nos players mundiais.

Resumindo, acho que então para uma empresa que, e agora estou a falar um bocadinho sob o chapéu da minha empresa, opera exclusivamente no espaço europeu e cuja atividade é alvo de regulação, como é o caso das comunicações eletrónicas, e o próprio tratamento da informação é fundamental para a disponibilização dos produtos e serviços, achamos e consequentemente para garantir uma experiência do cliente excecional, ou pelo menos boa, muito boa, otimizada, então nesse sentido acho que a concorrência sã e com regras muito claras e transparência, ajuda bastante neste jogo em que estamos. Independentemente de a empresa estar dentro ou fora do espaço europeu.

(Empresa C) Isto da proteção de dados, ou da legislação para a proteção de dados, como é óbvio, estava a ser preciso. Eu acho que aqui nenhum profissional, nenhum marketeer, nenhuma pessoa que trabalha no ramo, dirá que foi totalmente desnecessário. Chegou a um ponto em que efetivamente começava a ser um caos a forma como os dados dos clientes eram tratados, o que é que faziam com eles, ou seja, foi totalmente necessária e se calhar até já veio um pouco fora de tempo. Porque quando veio, as coisas já estavam tão desreguladas e tão pouco claras, tanto para o consumidor como para a empresa, o que fez com que a implementação depois fosse muito difícil porque deixamo-nos até a um certo nível em que depois ter que voltar atrás foi bastante mais difícil do que se nunca tivéssemos chegado a esse nível. Por isso eu acho que foi sem dúvida necessário e aqui em termos de legislação as empresas tiveram mais do que tempo para se adaptarem. Mas como todo o ser humano, depois acabou tudo por ser feito em cima da hora e só quando as coimas começaram a ser aplicadas e a legislação entrou efetivamente em vigor, é que houve por parte essa preocupação e essa prioridade nas medidas.

No nosso caso, obrigou a muito. Ou seja, em 2018, a legislação já saiu, salvo erro, agora posso estar um bocadinho enganada nas datas, mas se estás a aprofundar um tema saberás melhor do que eu, a legislação já saiu em 2015 ou 2016, e a aplicação seria só passado dois anos. Ou seja, efetivamente deram dois anos às empresas, mas posso-te dizer que, no caso da Salsa, nós começamos a trabalhar na implementação meses antes da data de 2018 e não logo quando começou a ser público que iria acontecer. Por isso foi um projeto bastante duro, na perspetiva

que teve também de ser feito em tempo recorde, e que levou a muitas alterações. Ou seja, exemplos práticos da Salsa:

Nós ainda tínhamos, naquela altura, o registo dos clientes, principalmente no retalho físico, em formato de papel, ou seja, o cliente preenchia a típica ficha de papel e depois o colaborador passava esses dados para o computador. Tínhamos um arquivo central onde guardávamos essas fichas, mas que fazer o trace disso era perto de impossível. Se um cliente, à luz deste novo regulamento exigisse a prova que efetivamente fez a inscrição, eram caixas e caixas e caixas de folhas de papel o que tornava quase impossível termos a prova que efetivamente ele nos deu essa autorização e que nos facultou os seus dados. Por isso, como esta legislação obrigava a isso, tivemos de acelerar aqui o que já era um objetivo: eliminar o papel e tornar a empresa muito mais digital. Mas tivemos que acelerar a passos largos esse objetivo e garantir que a inscrição dos clientes nas nossas lojas era feita digitalmente e não por papel. Obrigou a alguns desenvolvimentos a nível de IT porque tivemos de preparar uma espécie de aplicações para o cliente se poder registar em loja. O formato de consentimento que encontramos, ou que achamos que na altura facilitava a experiência do cliente e conseguíamos gerir, era o processo de assinatura digital. Ou seja, o cliente que até então assinava numa folha de papel, passava a assinar num ecrã. O que também trouxe aqui uma carga adicional de investimento, que foi dotar todas as nossas lojas de um equipamento no qual fosse possível os clientes assinarem digitalmente. Mas foi essa a evolução que fizemos no processo de captação de dados para garantir que, de alguma forma, digitalizávamos essa informação e ao digitalizá-la teríamos essa informação disponível para acesso para quando o cliente assim exigisse a prova, ou quando outras autoridades também processos de auditoria ou outros tipos de processos, exigisse a prova de consentimento dos nossos clientes.

Na captação de dados foi este o impacto no retalho físico, teve impacto no digital porque também nos obrigou a tornar o processo de registo mais complexo, porque a questão de confirmar os dados do cliente, termos a certeza de que estamos a captar esses dados levou a que tivéssemos de rever alguns formatos de como estávamos a angariar. Isto tanto no nosso próprio site como também parceiros.

E no caso dos parceiros ainda foi mais relevante porque depois quando falamos em marketing digital e de angariação de leads, em que nós pagamos aos parceiros, ou os parceiros são remunerados pelos contactos que nos fazem chegar, quanto mais complexo é o processo, menos contactos nos chegam e eles também vêm de alguma forma alguma quebra do sucesso da campanha de angariação. Mas este foi um dos pontos que tivemos obrigatoriamente de cumprir.

Depois também tivemos que desenvolver/melhoras muitas ferramentas internas para conseguir cumprir todos os pontos relativamente à privacidade dos dados. (..) ferramenta que só vê dados pessoais de cliente. Eu estou aqui a focar-me muito no cliente, porque efetivamente é a alçada que está sobre a minha responsabilidade, mas o GDPR aplica-se tanto a clientes, como a fornecedores, como colaboradores. Ou seja, abarcou todo o espectro de dados pessoais. Mas no caso dos clientes também tivemos que, nas nossas ferramentas internas de alguma forma criar acessos diferenciados – ou seja definir quem é que efetivamente precisava de aceder à informação dos clientes e para quem é que informação que nós chamamos de informação anonimizada seria mais do que suficiente. Ou seja, se eu só quero ver compras e analisar vendas, não me interessa saber se é da Maria ou do Manel. Só quero saber se aquele cliente fez compras. Por isso toda a nossa estrutura de dados teve de ser organizada nesse sentido para que

só mesmo situações que implicassem tu saberes que estás a falar com aquele cliente, com o número de contacto associado, é que efetivamente teriam acesso a esses dados. Ou seja, passamos praticamente de toda a empresa ter acesso aos dados dos clientes passou a só quase a equipa de apoio ao cliente, porque é quem efetivamente precisa de fazer esse apoio micro – esse apoio de saber com quem está a falar e informação única do cliente -, a ter acesso a essa informação, e todas as outras áreas em que apenas trabalhavam resultados, números e afins apenas viam dados anónimos e não informações específicas. Isto também foi um grande projeto de reestruturação.

E depois se calhar aquele que para nós foi mais complicado, na perspetiva que havia tantas opções de como fazer isto, e tão poucas soluções de mercado, que nós acabamos por ter de desenvolver a nossa própria solução, que tinha mais a ver com a retenção dos dados. Porque outra coisa que o GDPR também trouxa foi datas de validade. Ou seja, nós antes angariávamos um dado cliente, e ficávamos com ele para sempre sem grande tema. O que o GDPR trouxe foram validades – eu só posso manter aquela informação durante determinado tempo, e tendo em conta o tipo de informação esse tempo também varia. E depois, dentro da legislação, e foi aqui uma carga legal bastante forte que pelo menos eu tive que conhecer e analisar entre o que está na legislação e o que efetivamente cada empresa pode aplicar vai uma grande distância. São tantas as opções, que eles até sugerem que pode ser isto, mas depois o negócio tem as suas especificidades, a informação é necessária para uma dada finalidade ou é preciso realizar este tipo de ações sobre esta informação, e que pode levar a outro tipo de validades/retenção. Depois também se impunham as retenções legais, porque nós somos uma empresa que vende serviços, ou seja, fatura serviços, então legalmente perante a autoridade tributária eu tenho de reter informação durante determinado tempo, mas esse tempo não é justificação para eu reter para outros fins. Ou seja, eu tenho de reter a questão da faturação, mas a questão de outra informação já não é justificação. Os advogados/entendidos da matéria já defendem que não precisamos de reter durante tanto tempo isso para fins de Marketing. Ou seja, precisamos para fins fiscais, mas para fins de marketing já não pode ser esse período de tempo. Então, obrigou quase a criar aqui layers de retenção de dados, em que numas plataformas eu apago passado um tempo, noutras plataformas eu apago passado outro tempo. No meio disto tudo, se o cliente me disser para não apagar, eu não posso apagar, o que criou ainda este nível de complexidade em cima.

Isto tudo são projetos que envolvem uma grande complexidade operacional, mas principalmente técnica, e que para o cliente são pouco visíveis. Porque há aquele cliente mais informado, mais complexo que até quer saber como isto funciona e nos pede essa informação. E existem. Na altura, em maio de 2018, existiram bastante clientes, até porque os telejornais não paravam de falar nisso e houve até vários pedidos de cliente a querer saber como é que nós geríamos a informação deles, como é que guardávamos, onde guardávamos… quase a fazer um levantamento de todos os direitos que tinham acesso. A verdade é que, depois disso, eu posso dizer que hoje, à nossa magnitude que temos de mais de um milhão de clientes, recebemos este tipo de pedidos relacionados com GDPR numa escala de dois ou três por semana. Ou seja, um projeto daquela magnitude e com aquele investimento tudo, como é óbvio tínhamos d estar compliant e tínhamos de seguir as regras, mas depois na realidade a perceção do consumidor final para aquilo é reduzidíssima. Eu acho que quando as empresas não estão a cumprir, ou quando não estão a usar a informação de forma consciente e forma transparente, é gritante, ou seja, o consumidor percebe que do nada deu o seu e-mail para aquilo e foi parar

não sei onde. Mas quando as empresas já tinham pouco esse cuidado e essa preocupação, ter que implementar toda esta robustez de informação por cima, foi sem dúvida um grande projeto e um investimento muito grande que não trouxe retorno. É impossível um investimento destes trazer retorno financeiro porque não é percebido pelo cliente. Ou seja, eu não melhorei a eficiência do cliente.

2. O que foi feito dentro da sua empresa para se prepararem para a implementação do RGPD?

(Empresa A) Sendo a GNG uma empresa especializada em retalho, os serviços legais e jurídicos são subcontratados. Com o surgimento de um novo enquadramento legal que afetaria pelo menos uma parte da atuação da empresa, a primeira decisão foi, naturalmente, a alocação – também num regime de consultoria – de uma equipa legal ao processo de transição em inícios de 2017, que teve como objetivo fazer o levantamento dos processos existentes, traçar o plano de ação que visava a transformação necessária para acomodar todos os fluxos de dados existentes à luz da nova legislação, programar e detalhar a sua concretização e, numa fase posterior, acompanhar e auditar a sus implementação.

Uma das primeiras conclusões desse trabalho foi a identificação da necessidade, face à complexidade e abrangência de atuação da empresa, da nomeação de um Data Protection Officer (DPO, ou EPD em português), para liderar o projeto internamente e assegurar a continuidade da monitorização a aplicação das políticas definidas para além do prazo do projeto.

(Empresa B) Ora bem, a conformidade com o RGPD era assente no cumprimento dos princípios fundamentais no tratamento dos dados pessoais e na garantia de isso existir é … toda a cadeia de valor, certo?

Portanto, por outro lado, e como mencionou, o setor das comunicações eletrónicas, está sujeito a uma legislação própria que é a lei 41, que até está prevista ser alterada (estamos a aguardar pelo regulamento do e-Privacy, não sei se lhe é familiar, e esta legislação, quer o artigo 67, quer esta nova lei 41, já contempla os direitos dos titulares, portanto não é uma coisa nova. Já contempla alguma gestão, nomeadamente os consentimentos, já menciona também os prazos de retenção, e medidas de segurança.

Face à base que nós tínhamos e àquilo que o RGPD nos trouxe de novo, então quais foram essas novidades? E de facto tivemos que fazer no sentido de dar resposta.

Primeiro a nomeação de um responsável para a Proteção de Dados. Uma figura que nós não tínhamos dessa maneira. Tínhamos de facto uma figura de destaque no que se refere à conformidade com os dados pessoais, mas não era sobre a forma de Encarregado de Proteção de Dados, que é uma figura que supervisiona a aplicação do regulamento dentro da própria empresa, articula com as autoridades de controlo, e também com os titulares, sobretudo no caso de violações de dados e consequentemente na implementação dos processos associados, como as reclamações.

Depois também tivemos, do ponto de vista dos direitos dos titulares, fazer algum reforço de implementação de direitos, tais como melhorar a informação aos titulares sobre os tratamentos efetuados e também ajustar os consentimentos que já tínhamos em função dos regulamentos e dos processos associados ao tratamento desses mesmos consentimentos e todas as finalidades

Depois, do ponto de vista de parceiros, de sub-contratantes, que o RGPD valoriza, tivemos que celebrar junto dos sub-contratantes, acordos de tratamento de dados. Portanto os contratos que nós tínhamos ou as políticas que até partilhávamos com os nossos parceiros, não era suficiente face àquilo que o RGPD exige. Porque tivemos de estabelecer o acordo de tratamento de dados porque os mecanismos que existiam não estavam a cumprir a parte do regulamento e tivemos de evoluir nesse sentido. Porque os acordos, indicam as finalidades, que os tratamentos de dados são apenas para as finalidades estabelecidas no acordo, às medidas de segurança que são necessárias ter, e algumas instruções específicas dependendo da natureza do tratamento que faz.

Depois também tivemos que implementar o registo das atividades de tratamento de dados – às quais chamamos internamente RATs. Também a parte da avaliação de risco – quando o risco é mais elevado fazer os Privacy Impact Assessments, os P's, e também reforçamos algumas coisas de segurança.

Depois também tivemos de alterar os processos de desenvolvimento para terem uma natureza mais privacy-by-default (no sentido do tratamento dos dados estritamente necessários para a finalidade específica e pelas pessoas para as quais é essencial ter acesso e depois também pelo prazo mínimo indispensável para concluir o tratamento) e privacy-by-design (a aplicação dos meios de segurança técnicos depois na origem)

Há duas vertentes: a primeira, direitos e consentimentos, a verde do lado direito, e depois há a auto-regulação. Dentro das medidas de direitos e consentimentos nós tivemos logo que fazer o reforço e alguns direitos novos – prestar informação transparente, o exercício dos direitos (acesso, portabilidade, retificação, pagamento, limitação e oposição), a questão do direito de reclamar sobre o modo como os dados pessoais são tratados ou o encarregado de proteção de dados e a autoridade de controlo e depois também serem informados sobre as violações, no caso dos titulares. Na parte dos consentimentos, ou se obtém o consentimento para os tratamentos, se estes não assentarem em interesse legítimo, obrigação legal ou execução de contrato. O consentimento deve ainda ser livre, informado, específico, expresso e evidenciável. Isto do lado do direito. Importante referir também que o titular não é só o cliente. O colaborador também é titular, o colaborador parceiro também é titular…

Na parte da autorregulação, começa logo com a organização, com o DPO, depois também a parte do tratamento, em que nós temos de facto de fazer o registo e perceber de que maneira é que tratamos os dados, quer seja através dos RATs, avaliações de risco – temos dois instrumentos para isso: uma avaliação de risco por defeito e outra para quando o risco é alto. Depois também se implementam as medidas de segurança.

Na parte de desenvolvimento temos o privacy-by-default e o privacy-by-design, e toda a parte de tratamento de dados com a formalização da relação com os subcontratantes.

3. Que efeitos positivos o RGPD teve na sua organização?

(Empresa A) Conforme já referido, a análise e transformação todos os processos de informação e comunicação da empresa de modo estruturado e sistematizado traduziram-se num melhor conhecimento e controlo internos, tornando esses processos melhor documentados, mais robustos e seguros.

Outra vertente relacionada que acabou por se revelar sinergética e ter um impacto extremamente positivo na empresa foi o projeto de segurança informática lançado na sequência de recomendações originadas pelo levantamento/análise de processos anteriormente descritos; projeto esse que levou a que fosse paralelamente feito um levantamento técnico das soluções informáticas (infraestrutura, arquitetura de redes, etc.) e a sua adaptação à nova realidade ditada não só pelos requisitos presentes no RGPD, como à crescente digitalização e aposta em comércio eletrónico e tecnologias de informação em geral.

(Empresa B) Começando pelos positivos, acho que tudo aquilo que falamos até agora, e reforçado, como já disse pelas ações de formação interna e o próprio awareness público que tem vindo a crescer e criou-se uma grande expectativa do ponto de vista da opinião pública sobre ao RGPD. Isto permitiu tornar a organização ainda mais consciente e conforme ao tema da privacidade e do tratamento de dados pessoais para os clientes e também para os diferentes tipos de titulares. Isto à partida são os aspetos positivos.

4. Que efeitos negativos o RGPD teve na sua organização?

(Empresa A) Dada a natureza preparatória do projeto, executado em antecipação à aplicação da nova legislação, não se pode propriamente falar em efeitos negativos continuados na organização, até porque o trabalho realizado consistiu precisamente em garantir a manutenção das operações da empresa, preparando-as gradualmente para o total cumprimento do novo quadro legal. Naturalmente que houve dificuldades inerentes à implementação, entraves momentâneos, dores de crescimento e custos associados, mas não se pode falar em efeitos negativos que tenham perdurado para além da fase de implementação.

(Empresa B) Relativamente a aspetos negativos, a longo prazo, não identificamos nenhuns aspetos negativos relevantes. O que observamos foi uma maior carga administrativa. Todos os processos foram montados - nem sempre havia aplicações já prontas para responder automaticamente, mas que ao longo do tempo temos feito o trabalho de criar maior automatismo, portanto mesmo essa carga administrativa tem vindo a diminuir. Mas não acreditamos que exista um aspeto negativo o longo prazo que consiga apontar.

5. Como é que o RGPD mudou a vossa estratégia, se o fez?

(Empresa A) A publicação e posterior aplicação do RGPD não mudou, de facto, a estratégia da empresa. A GNG sempre encarou os dados e o conhecimento digitais como o principal fator para o aporte de valor num setor tão competitivo como o retalho, pelo que sempre procurou e continuou a procurar explorar da melhor maneira as potencialidades presentes nos dados, à luz da sempre-crescente panóplia de tecnologias emergentes para o seu tratamento. Prestar um serviço de excelência, personalizado e que vá de encontro às necessidades do consumidor foi, ao longo de todo o processo, um dos pilares de atuação da empresa, e isso de facto não mudou. O RGPD representou um ponto de referência, de atuação e de implementação técnica, para que a empresa continuasse a perseguição dos seus objetivos, e não um entrave nesse sentido.

(Empresa B) A estratégia da nossa empresa assenta fortemente na satisfação do cliente e na confiança. O que também é comum, espero eu, à maior parte das empresas. A privacidade entendemos que é um dos pilares essenciais na construção dessa relação de confiança. Portanto esta implementação foi um influenciador positivo ao nível da privacidade, mas também ao nível da segurança. Porque segurança e privacidade não são indissociáveis.

(Empresa C) Eu acho que aí mudou o mindset. Agora cada vez que criamos ou desenvolvemos alguma coisa, já o fazemos com alguma preocupação sobre o tema e como é óbvio trouxe, embora na Salsa a orientação para o cliente já é um pilar da empresa e todos os colaboradores têm isso bem vincado, mas sempre foi uma orientação para a experiência do cliente. E com todas estas alterações que tivemos de fazer e todas estas legislações que foi colocada em cima, além de uma orientação para a experiência também trouxe uma orientação para a privacidade, para ter a certeza de que quando construímos coisas ou quando criamos serviços - quando alteramos modelos de atendimento, por exemplo -, quando fazemos este tipo de abordagens, já o fazemos tendo consciência destes dois fatores: tanto a experiência como a privacidade e a segurança da informação do cliente. E eu acho que isso é sem dúvida uma coisa positiva e um plus para nós porque também nos ajuda na credibilidade para com o cliente, na proximidade e confiança. E acho que isso foi uma mais-valia e uma alteração na forma como estavam a ser feitas as coisas. Antes era mais "vamos fazer e depois vemos como é que resolvemos esses temas de informação e tudo mais", e agora passou a estar na própria criação e idealização já existe essa preocupação.

Acho que não via ficar por aqui em termos desta legislação, até porque para mim ela teve muitas lacunas e por isso é que já surgiram outras, entretanto a nível da privacidade online. Aqui trabalhou-se muito a nível dos dados pessoais do cliente, coisas tangíveis (o meu nome, o meu email, o meu telefone) e tudo mais, mas deixou de fora ou pelo menos não regulou de forma muito exata, porque levou a várias interpretações de diversas formas, relativamente à minha presença online e à minha identificação online. Tanto que depois disse já surgiu uma lei de cookies, já surgiu uma lei de privacidade e cibersegurança, e todas estas que acabaram por ser, na minha opinião, remendos em cima de uma legislação de base em que ainda há muitas zonas cinzentas. Ainda há muitos pontos, e focando um bocadinho nas cookies que se calhar é o exemplo mais específico – para que é que efetivamente as empresas estão a usar a tua

informação online, ou seja o teu tracking? Para que é que estão a fazer tracking de ti quando estás a navegar e onde estás a operar? Isto é ainda muito cinzento o que para mim é publicidade e para outros é análise. O que eu digo que estou a fazer para melhorar os meus serviços e os meus produtos com base no teu perfil, outros dizem que estão a fazer isso para depois te poderem fazer publicidade noutros sites. Ou seja, ainda há aqui uma zona muito cinzenta dos fins para os quais estamos a recolher e acompanhar a informação a esse nível. Já não é tanto um tema que o GDPR cobria, porque o GDPR cobria coisas mais tangíveis, coisas como quem eu sou, o meu nome e a minha morada, mas eu acho que é cada vez mais invasão da minha privacidade isto do que outras coisas. Ou seja, saberem onde eu estou, saberem o que eu faço, saberem que todos os dias à mesma hora eu vou a determinado site, acho que acaba por atacar mais a privacidade das pessoas do que outras coisas. E este sim, e já está a ser regulado, inclusive há pontos que já estão a ter bastante impacto no dia a dia das empresas. Mas quando eles restringirem mais e forem mais explícitos do que realmente é uma coisa e no que realmente é outra, e a aposta cada vez maior que está no digital e na publicidade e na experiência digital, eu acho que aí sim, vai ter bastante mais impactos. E no caso da Salsa, eu diria que financeiros, em termos de perdas de receita e afins, vai ter mais impacto estas legislações de cookies, legislações de privacidade e legislações da identificação dos clientes online, do que propriamente teve o GDPR. O GDPR teve muita burocracia e muitos custos de implementação, mas como nós, mesmo podendo não ter as coisas direitinhas, mas já sabíamos o que podíamos ou não podíamos fazer para o cliente, a diferença não muita. Ou seja, não sentimos aí uma quebra muito elevada nos clientes que contactávamos, nos clientes que podíamos enviar sms, nos clientes que podíamos enviar newsletters, porque nós já tínhamos essa parte mais ou menos registada e bem construída. Esta componente online é que acho que vai trazer outros desafios, porque inclusive as ferramentas funcionam assim, ou seja, tu fazes publicidade com base em comportamentos e nas análises que foram feitas a esse comportamento, e se tu deixares de poder analisar comportamento, deixas de poder fazer publicidade. E nessa parte, é que financeiramente, já estamos a ver alguma quebra quando já tens googles e facebooks a bloquear coisas e acho que vai ser cada vez pior e essas próprias ferramentas e motores vão ter de se reinventar para continuarmos a conseguir cumprir os objetivos. Porque depois tens por um lado, a tendência é a personalização, é tu conseguires dar ao cliente aquilo que quer, à hora que quer e quando quer, mas se tu não souberes quando isso é, nunca vais saber unir os dois objetivos. E por um lado, eu dizia isto muitas vezes, o cliente quer personalização, mas depois não quer dizer quem ele é, o que gosta e o que faz, e assim é impossível.

6. Que custos adicionais teve a implementação do RGPD na vossa empresa?

(Empresa A) Toda a fase de preparação para a aplicação do RGPD, que decorreu nos moldes já mencionados, representou um investimento em dois projetos quase paralelos (legal/jurídico e técnico/informático): ambos efetuados em regime de subcontratação de serviços de consultoria, com alocação de um gestor de projeto interno que ficou responsável pela alocação de tarefas internamente, permitindo à empresa efetivamente operar a mudança com elementos internos sob orientação de especialistas externos. Ambos os projetos tiveram a duração de sensivelmente um ano, tendo o projeto jurídico/legal prosseguido até à data sob a forma de

horas para aconselhamento e steering para fazer face às correntes/futuras interpretações e retificações/alterações do regulamento.

(Empresa B) Fizemos o que era necessário, e investimos o que era necessário.

(Empresa C) Eu acho que houve um investimento comum. Acho que todas as empresas terem feito, e foi por isso é que eu também estava a dizer no início que foi um bem ou mal necessário, e haver uma legislação, tornou os consumidores mais tranquilos relativamente a quando estão a partilhar os dados, ou pelo menos já o fazem e não têm tanto receio relativamente do que vai acontecer com isso. Sem dúvida que para o bem maior, acho que esta legislação veio garantir que todas as empresas implementam as regras e trouxe sem dúvida um bem maior para o mercado e para a economia num todo. A nível individual da empresa, não creio que algum dia um projeto deste tipo possa ser considerado como um retorno positivo. No entanto, é algo que tinha de ser feito. E por essas razões é que a maior parte das empresas acabou um bocadinho por ser como nós, ou seja, tentou empurrar ao máximo este tipo de desenvolvimentos e este tipo de ações que tinha que tomar porque sabia que nunca eram prioritárias versus outras coisas que poderiam contribuir muita mais a curto prazo ou médio prazo para o negócio. Mas sim, esse ponto não tenho qualquer dúvida. Tornou o mercado muita mais confiável. Não é um canal que a Salsa tenha, ou utilize, mas conheço porque em anteriores funções já tive nesse ramo, ou pelo menos acompanhava de alguma forma esse ramo, mas até várias estruturas e empresas de telemarketing acabaram por não resistir porque efetivamente eram esses setores que andavam a abusar um pouco da constante partilha e flexibilização de dados pessoais dos clientes. Embora algumas ainda se mantém e continuem de alguma forma a fazer negócio com isso, a verdade é que a maior parte acabou por não conseguir vingar porque garantindo todas estas políticas e medidas de segurança, eles perderam muito potencial de contacto e de venda. Se calhar isso era a face mais gritante para o consumidor – ou seja, era do género: "está-me a ligar esta empresa e não faço a mínima ideia de quem ela é e como é que realmente chegou ao meu número de telefone, ou chegou ao meu email". Era este ponto que tornava pouco credível a segurança nos dados que existia.

7. Na perceção da sua empresa, o que pensa que o RGPD pode melhorar de forma a minimizar os impactos negativos que mencionou?

(Empresa A) Não tendo impactos negativos a apontar no ponto 4, e de acordo com a posição da GNG anteriormente referida perante o RGPD, este é por nós visto como uma ferramenta que visa garantir a uniformidade/equidade no tratamento de dados pessoais, assim como a preservação da privacidade do indivíduo, pelo que não nos merece qualquer tipo de consideração nesse âmbito.

(Empresa B) Como falei, apenas considero esse aspeto negativo a curto prazo. Como não consideramos nenhum efeito negativo a longo, não interessa a ponto de necessitar uma mudança no RGPD. Acho que as coimas se afiguram muito avultadas.

(Empresa C) Eu nem te vou responder muito bem o que é que deveriam ter no GDPR, eu vou dar um bocadinho volta à pergunta. Porque efetivamente a preocupação dos governos é a

mesma de toda a gente, no entanto eu só acho que deveria haver maior preocupação com a parte do acompanhamento e do follow-up e do seguimento. Ver efetivamente quais são as marcas que não estão a cumprir e por vezes criam restrições e legislações muito rígidas em que mesmo quem cumpre tem muitas dificuldades em as garantir, enquanto a preocupação deveria ser um pouco mais flexibilizada, garantindo depois fazem o acompanhamento e que as marcas e as empresas cumprem esses requisitos. Porque por vezes acabam por se fazer legislações tão complexas que ficam possíveis de implementar a 100%. E poderiam de alguma forma flexibilizar se depois de alguma forma conseguissem garantir, o que também é um problema, visto que a autoridade da proteção de dados tem recursos escassos para andar a fazer follow-up e a ver efetivamente quais são as empresas que estão a cumprir e que não estão a cumprir, e depois acabam por funcionar apenas por queixas, por reclamações. E aí sofrem os grandes que efetivamente quantos mais clientes têm, mais reclamações vão ter e se calhar são as empresas mais pequenas que podem se calhar estar a fazer mais mal à forma como lidam com os dados.