

# Vivo ou morto, quem <sup>1</sup> pode ver as mensagens que envio e recebo na Internet? /premium

15 Agosto 2018



Manuel Pestana Machado

"Acederem ao meu Gmail é acederem à minha vida."

Seja um Observador /premium

seus dados pessoais em emails, redes sociais e apps de mensagens, durante a vida e depois da morte.

Partilhe     

- 1 [Em que situações podem ler o meu email e aceder ao meu WhatsApp?](#)
- 2 [Preparar o meu testamento digital](#)
- 3 [O Facebook e o Memorial que fica para os amigos](#)
- 4 [Há apps a verem o que faço online](#)

A dúvida instalou-se quando o Supremo Tribunal Alemão decidiu, em julho deste ano, que [os pais da adolescente de 15 anos que morreu em 2012](#) podiam aceder à conta que esta tinha no Facebook. Objetivo: verificar se a sua morte terá resultado de um acidente ou de suicídio. A empresa foi obrigada a dar acesso aos pais, apesar de ter contestado que isso violava o direito à privacidade. À Reuters, Ulf Buermeyer, ativista de direitos sociais alemão, contra-argumentou: “Enquanto os pais tiveram de perder anos no tribunal para poderem ler as mensagens da filha, a NSA e os Serviços Federais de Inteligência [alemães] conseguiram-no fazer com apenas uns cliques do rato”. Afinal, quem pode aceder aos dados pessoais de um utilizador enquanto este está vivo e depois de estar morto?

Os emails e escutas telefónicas são cenários para os quais a Polícia Judiciária e os tribunais estão preparados, mas interceptar chamadas de WhatsApp e ter um quadro legal que estabelece quem pode aceder a dados pessoais (e como) depois da morte são áreas que em Portugal ainda não têm regulamentação. Mesmo assim, há empresas que conseguem aceder a estes dados sem enfrentarem muitos problemas, graças a aplicações que desenvolvem para esse efeito. Uma coisa é certa, explica o advogado David Silva Ramalho: “Acederem ao meu Gmail é acederem à minha vida, não é comparável a uma busca à minha casa”.

## Em que situações podem ler o meu email e aceder ao meu WhatsApp?

A palavra-chave para se poderem ler emails e mensagens de plataformas como o Gmail, Hotmail, Facebook, Messenger ou WhatsApp é “consentimento”. Para aceder a cada programa, o procedimento técnico final é diferente e, mesmo sem consentimento, as autoridades podem ver os seus dados pessoais, se considerarem que há um motivo forte para o fazerem. A questão que fica é: como é que o fazem? Em Portugal, há procedimentos para se fazerem “escutas” a chamadas, interceptar SMS e apreender emails, mas o caso fica mais difícil com aplicações como o Facebook Messenger e o WhatsApp.







Na Europa, o WhatsApp não pode partilhar informação de utilizadores com a empresa que o detém, o Facebook. Em causa está o cumprimento das normas de proteção de dados e expectativa dos utilizadores

“Podem ver o seu email aqueles que tenham acesso à password [palavra-passe] do mesmo”, explicou ao Observador Armando Dias Ramos. É inspetor chefe na Polícia Judiciária, professor adjunto convidado no Instituto Politécnico de Beja e autor do livro “A Prova Digital em Processo Penal: o Correio Eletrónico”.

“Há dois tipos de email: aquele a que se tem acesso apenas a partir do computador, quando as mensagens são descarregadas do servidor da empresa, usando programas como o Outlook por exemplo, e os chamados Webmails, como o Gmail e outros, cujas mensagens não são descarregadas do servidor e às quais podemos aceder em qualquer dispositivo com acesso à Internet”, explicou o inspetor da PJ.

Quem determina que se pode ler o email de alguém? “Apenas um juiz tem a autoridade para apreender o correio eletrónico”, esclarece David Silva Ramalho, advogado na Morais Leitão e especialista em Cibersegurança e Proteção de Dados. “Frequentemente, o Ministério Público faz uma comparação com o regime das cartas físicas”, refere o jurista, advertindo que esta situação tem criado diversos problemas, porque são “realidades diferentes”. Um dos casos é o tal acesso a Webmails. Quem acede a uma conta de email através de um browser está a receber dados alojados em servidores que estão fora do país. “Afeta a soberania de outro Estado”, argumenta o advogado.

“A polícia pode aceder à informação que está no computador, mas o que é desejável é copiar literalmente o computador para evitar contaminar a prova. Outra alternativa são os *live forensics* [aceder diretamente ao computador para encontrar a informação] (como permite o artigo 15, número 5 da Lei do Cibercrime)”. É nesta última situação que se cria o problema, porque alguém que tem um mandado para aceder a um email num computador, com palavra passe, acede a informação que está alojada noutros estados e, mesmo sendo permitido pela lei do Cibercrime, vai contra a norma internacional, a Convenção sobre o Cibercrime.

"A polícia pode aceder à informação que está no computador, mas o que é desejável é copiar literalmente o computador para evitar contaminar a prova"

David Silva Ramalho, advogado na Morais Leitão & Associados

Contudo, mesmo obtendo uma ordem judicial, a verdade é que sem *password* não se consegue fazer muito, explicam. No caso dos emails que são pirateados, como disse Armando Dias Ramos, o que acontece é “o acesso aos webmails ser realizado em pontos wi-fi que não são fidedignos e, a partir daí, podem ‘snifar’ os dados de acesso e ter acesso ao mesmo”. Ou seja, o princípio passa por conseguir a chave para depois poder entrar na casa e não arrombar a porta (porque é mais fácil roubar a chave).

Em Portugal, só quando está em causa um processo criminal é que podemos aceder a estes dados de forma coerciva, mas não vale tudo e o tema cria debate entre juristas, como diz David Silva Ramalho: “Há divisão na doutrina. Posso ser compelido a facultar a minha palavra passe?”. É que para o advogado, quando se faculta a palavra-passe viola-se o “direito à não incriminação”. Por isso, não se pode acusar de obstrução à Justiça quem não quiser fornecer a sua password. “A polícia normalmente pede, mas não obriga. Se o arguido não der, não tem consequências”, conta o advogado.

Depois de as autoridades conseguirem a palavra-passe, o processo para ler emails tem pouco de cinematográfico, como explica David Silva Ramalho: “Normalmente, [a busca] é feita por um perito da Polícia Judiciária. Senta-se à frente do computador e faz a busca com base em termos de pesquisa que, normalmente, são aprovados previamente. Depois, a polícia transfere para um disco externo”. Mas Dias Ramos deixa o aviso para as situações em que é preciso aceder a emails: “No fim, se o processo for público, qualquer pessoa com interesse legítimo pode ter acesso a todos os dados recolhidos”.



"Normalmente, [a busca] é feita por um perito da Polícia Judiciária. Senta-se à frente do computador e faz a pesquisa com base em termos de pesquisa que, normalmente, são aprovados previamente. Depois, a polícia transfere para um disco externo".

David Silva Ramalho, advogado na Morais Leitão & Associados

Como é que isto funciona em aplicações como as do WhatsApp ou do Messenger, que permitem fazer chamadas e trocar mensagens? "Por um lado, existe a criptografia [tecnologia que permite comunicação segura, para que não seja lida por terceiros] e, por outro, não estamos a falar de chamadas normais mas sim VoIP, ou seja voz sobre IP, isto é, não utilizam uma operadora mas dados de tráfego da Internet", explica Armando Dias Ramos. Numa escuta, um juiz pode permitir o acesso às chamadas e, depois, as operadoras gerem com a Polícia Judiciária a recolha das provas. Mas como estas aplicações funcionam por dados móveis ou Internet, a informação não passa pelas operadoras.

Não é por isso que é mais "seguro" utilizar estas aplicações. Como em Portugal apenas o Juiz de Instrução Criminal pode permitir o acesso a estes dados, depois o pedido tem de ser gerido entre a Polícia Judiciária e empresas como o Facebook e ou a Google (e não com as operadoras), que funcionam com ordenamentos jurídicos diferentes. Nestes casos, o *malware* ou "*software* espião", como conta o inspetor, "revelar-se-ia muito útil para a investigação criminal". Ou seja, os programas que permitem gravar à distância estas novas formas de comunicação em smartphones. "Em países como Espanha e Itália já se encontra legislada esta forma de atuação", explica Armando Dias Ramos. Mas em Portugal "não há previsão legislativa e, se alguém o utiliza, está a cometer uma ilegalidade, ou seja, a obter prova proibida."

Ao Observador, a Google esclareceu que tem um "relatório de transparência" relativo aos pedidos de informações provenientes de entidades sobre dados pessoais de utilizadores para todos os países. De Portugal, na última metade de 2017 (os dados são semestrais), houve **610 "solicitações de divulgação de dados de utilizadores" de 721 contas. No fim, 64% destes pedidos tiveram "alguns dados produzidos"**.

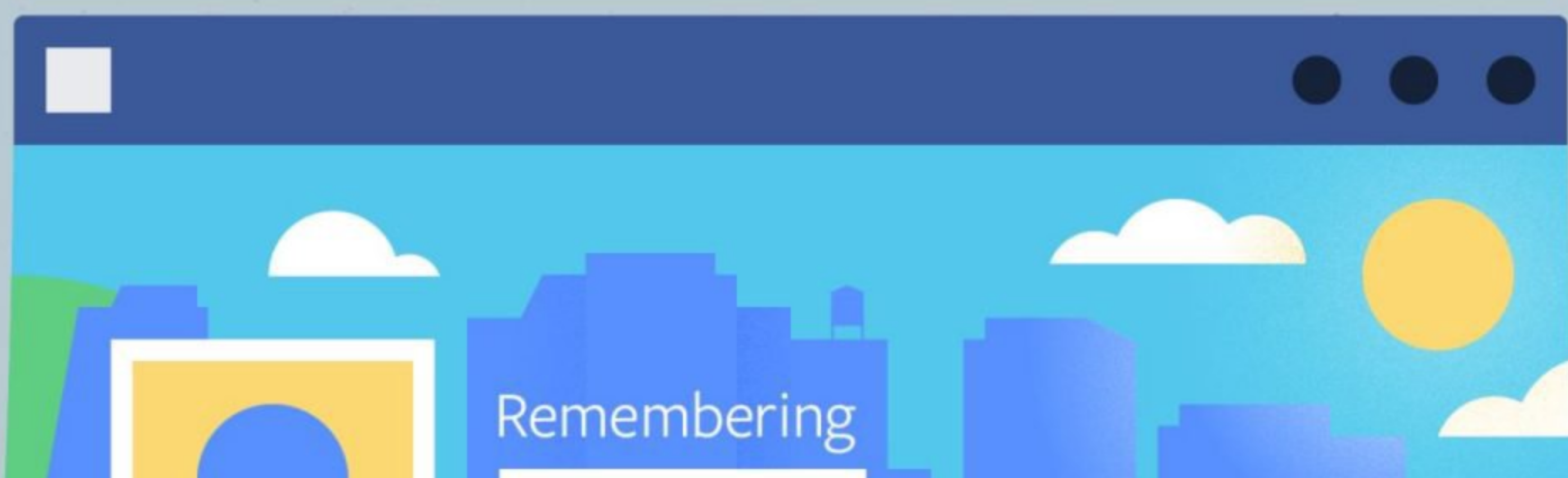
Nos casos de escutas ao Messenger e WhatsApp, o malware ou "software espião" "revelar-se-ia muito útil para a investigação criminal", admite o inspetor da PJ Armando Dias Ramos. Ou seja, programas que permitem gravar à distância estas novas formas de comunicação em smartphones.

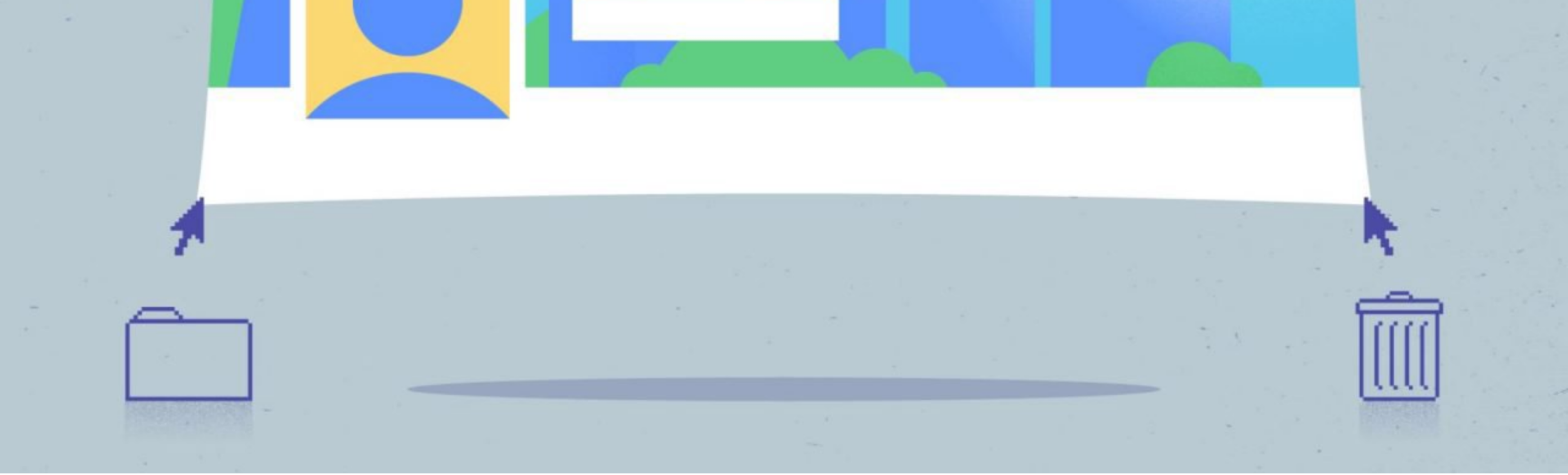
[Voltar ao índice](#)

### Preparar o meu testamento digital

Isto quer dizer que, desde que não existam suspeitas criminais sobre um utilizador, se este tiver cuidado e não tiver partilhado as suas passwords, o acesso às mensagens e fotografias está a salvo de olho alheio? No mundo digital, nunca nada é 100% certo, como comprovou o recente caso que envolveu a empresa de análise de dados britânica Cambridge Analytica e o Facebook.

E depois da morte? Mesmo "além da morte" há "reserva da intimidade da vida privada", adverte David Silva Ramalho. Já referimos o caso do Supremo Tribunal Federal Alemão, no qual uma mãe "herdou" a conta de Facebook da filha de 15 anos. O objetivo da família era descobrir se a rapariga se tinha suicidado, mas criou um precedente que provocou bastantes divergências. "Na Alemanha, comparam a entrega do Facebook à entrega de um diário, mas isso cria um problema: estamos a permitir o acesso à reserva da intimidade da vida privada de terceiros", argumenta o advogado. Podem existir casos em que haja "interesses preponderantes", mas o respeito pela vida privada costuma prevalecer.





No Facebook, depois de o utilizador morrer, a página passa a ter a referência: "Em Memória de"

Ou a situação "está contratualizada" ou, depois de morrerem, não há muito a fazer, porque em Portugal não há uma resposta para estas situações digitais, explicou o jurista ao Observador. Por isso, "o problema não se tem colocado muito além das seguradoras [que querem ter acesso à informação de pessoas mortas para justificar poderem não estar obrigadas a pagar montantes devidos]", explica David Silva Ramalho. Contudo, as principais empresas com acesso a grande volume de dados pessoais, como o Facebook e a Google, têm protocolos para estas situações que podem ser preparados durante a vida do utilizador.

[Voltar ao índice](#)

### O Facebook e o Memorial que fica para os amigos

No Facebook, há um memorial online. Desde fevereiro de 2015 que a empresa que detém as maiores redes sociais do mundo (Facebook, Instagram e também o WhatsApp) tem protocolos para o que acontece depois de o utilizador morrer. Se um utilizador [escolher](#) um "contacto legado" da sua rede de amigos do Facebook, após a morte a sua conta pode ser transformada num "Memorial" e o contacto escolhido pode marcar uma publicação no perfil da pessoa, responder a novos pedidos de amizade e atualizar a foto de perfil e a foto de capa.

Como [explica](#) o Facebook, este contacto pode gerir conteúdos da conta memorial e fazer download das fotografias carregadas para a rede social, mas não vai ter acesso às mensagens privadas que foram trocadas com outros utilizadores (quem as recebeu, contudo, continua a tê-las, neste caso, como uma carta). As mesmas opções são possíveis para o Instagram. Quem não quiser escolher alguém para gerir a conta depois de morrer ou, sequer, para manter o perfil ativo, [pode optar por avisar o Facebook que quer que a sua conta seja apagada após a morte \(um pedido que também pode ser feito pelos familiares\)](#). No entanto, se não houver nenhuma informação, a política é criar automaticamente uma página memorial.

Sobre a morte, a Google tem uma política diferente. "Reconhecemos que muitas pessoas morrem sem deixar instruções claras sobre como gerir as suas contas online", esclarece a Google [na página dedicada](#) a receber pedidos sobre contas de utilizadores falecidos. A empresa articula-se com familiares ou representantes de um falecido para fechar uma conta ou, em certos casos, fornecer o conteúdo de uma conta "após uma cuidadosa análise". Em qualquer caso, a Google garante que não fornece senhas de acesso dos utilizadores falecidos, para "manter as informações das pessoas seguras, protegidas e particulares."

Como a empresa também gere plataformas como o YouTube, Gmail ou Blogger, o mecanismo que permite garantir o que acontece após a morte do utilizador, conforme explicado pela empresa ao Observador, é o "Gerenciador de contas inativas". [Aqui](#), é possível deixar o contacto de "alguém de confiança" e definir que dados se partilham com esta pessoa escolhida (pode ir do acesso ao canal YouTube ao Gmail).

"Podemos trabalhar com membros imediatos da família e com representantes para fechar a conta de uma pessoa falecida, quando apropriado. Em certas circunstâncias, podemos fornecer o conteúdo da conta de um utilizador falecido. Em todos esses casos, a nossa principal responsabilidade é manter as informações das pessoas seguras, protegidas e particulares. Não podemos fornecer senhas ou outros detalhes de login. Qualquer decisão de atender a uma solicitação sobre um utilizador falecido será feita somente após uma cuidadosa análise."

Página oficial da Google

O Observador tentou contactar a Microsoft e a Apple, para saber que políticas pós-morte dos utilizadores têm, mas até à data de publicação



deste artigo não obteve resposta. Na Internet, a Apple informa que é necessário contactar diretamente a empresa para aceder aos dados da iCloud ou de um MacBook de alguém que já morreu. No caso da Microsoft, também é preciso pedir acesso à empresa (já no LinkedIn, detido pela mesma empresa, há uma [página para comunicar a morte de usuários](#) e apagar a conta). As duas empresas referem nos websites oficiais que, na maioria dos casos, apenas permitem o acesso a informação através de ordens judiciais.

Além disso, é possível deixar informações sobre como aceder e como devem ser tratados os dados digitais por familiares ou pessoas próximas, de outras formas seguras. Armando Dias Ramos admite que os “herdeiros legais possam aceder a dados digitais do defunto”, caso este lhes deixe, por exemplo, a password do Facebook. Neste caso, a empresa “nem iria perceber”.

[Voltar ao índice](#)

## Há apps a verem o que faço online

Se depois da morte, as respostas são ambíguas, durante a vida, os limites sobre aquilo a que podemos ou não aceder também não são claros. A lei pode ser clara quanto à obrigatoriedade do consentimento para aceder a dados pessoais de terceiros, mas como mostrou recentemente o caso que envolveu a aplicação da [La Liga](#), há apps que utilizam o microfone do smartphone para gravarem o som que os utilizadores estão a ouvir. E não estamos a falar de “software espião” utilizado para encontrar criminosos, como já referimos. No caso da app da La Liga, os responsáveis da liga de futebol espanhola alegaram que acediam ao microfone para tentarem descobrir emissões ilegais de jogos em bares.

Não são os únicos a recorrer a este tipo de mecanismo. Há programadores que estão a conseguir aceder a emails do Gmail, que os utilizadores julgavam ser confidenciais, como mostrou o [Wall Street Journal em julho](#). No final, a resposta da Google a esta polémica foi: “Mas deram consentimento” para que este acesso fosse permitido.

### La Liga: App usa microfone para ouvir utilizadores

Vários utilizadores da aplicação oficial da Liga de espanhola de futebol para smartphones revoltaram-se depois de saberem que a app acede ao microfone para captar som de emissões ilegais de jogos.



Por Manuel Pestana Machado

[Ler artigo](#) [Partilhar artigo](#)

OBSERVADOR

Não há dúvidas: “Tem de haver consentimento”, explica David Silva Ramalho. O problema nestas situações, nas quais as aplicações e programas acabam por ter acesso a informação pessoal, é que muitas vezes não é claro quem deu autorização. Este cenário leva a que, como contou o [El País](#) em agosto, milhões de utilizadores estejam vulneráveis só por instalarem uma app que julgavam ser inofensiva. Tal como aconteceu no caso que envolveu a Cambridge Analytica — os utilizadores achavam que estavam a fazer um teste de personalidade para fins académicos e os seus dados foram utilizados posteriormente para ajudar a eleger Donald Trump.

No início de agosto, o aviso veio da própria polícia espanhola: “Se descarregou alguma destas aplicações, elimine do seu dispositivo”. O apelo foi feito com base num [estudo da Adguard](#) (que disponibiliza uma extensão para *browser* como o Adblocker, para bloquear anúncios) divulgado em julho, e que levou as autoridades a darem vários exemplos de aplicações e extensões para browsers que vêem o que o utilizador faz — todas as apps que foram divulgadas (Block Site, Adblock Prime, Speed Booster, Battery Saver, AppLock, Clean Droid, Poper Blocker y CrxMouse) pertencem à mesma empresa, que está registada nos Estados Unidos da América, a Big Star Labs. Trata-se de aplicações para limpar espaço no smartphone, poupar bateria ou impedir anúncios nos *browsers*. Problema: além de fazerem o que dizem, vão um pouco mais longe e gravam todo o histórico de navegação dos utilizadores.

### 10 perguntas sobre a proteção dos (seus) dados /premium

Andou a receber e-mails por causa do novo Regulamento Geral sobre a Proteção de Dados (RGPD)? É porque passa a ser plenamente aplicável na União Europeia esta sexta-feira. Perceba o que está em causa.



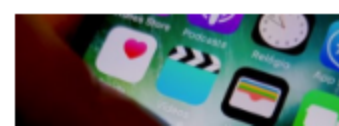
Por Manuel Pestana Machado

[Ler explicador](#) [Partilhar explicador](#)

OBSERVADOR

Para estes casos, o novo [Regulamento Geral sobre a Proteção de Dados \(RGPD\)](#), que passou a ser plenamente aplicável nos países da União Europeia desde 25 de maio, é claro: para aceder a estes dados é preciso o “consentimento explícito” dos utilizadores. O problema é que há várias aplicações que continuam a pedir o acesso a especificações dos smartphones que não parecem ser justificáveis. Por exemplo, se a uma aplicação de uma calculadora lhe pedir acesso ao microfone e à galeria de imagens, vai estar a pagar bem caro pelo que achou ser uma aplicação gratuita. O truque? Ver, através das definições do smartphone, que acessos foram dados à aplicação. Não consegue ver? Desinstale e instale outra vez e veja com atenção a que dados lhe pedem acesso.

### Programadores lêem os emails que troca no Gmail





Uma investigação do The Wall Street Journal concluiu que há centenas de programadores externos à Google que acedem aos emails trocados por milhões de pessoas no serviço de email da empresa.



Por Ana Pimentel

[Ler artigo](#) [Partilhar artigo](#)

OBSERVADOR

No caso da Google, as notícias revelaram que não eram apenas os algoritmos que “liam” os emails do Gmail, o principal serviço de correio eletrónico que detém mais de 1,4 mil milhões de utilizadores. Os colaboradores das empresas também o faziam. “Uma coisa é ter um *bot* para facilitar as pesquisas ou fins de marketing automático, outra é existirem humanos a lerem dados pessoais”, compara David Silva Ramalho.

Neste caso, a empresa explicou que parou de ler o correio eletrónico de terceiros, mas a verdade é que existem aplicações que podem ter acesso aos dados se os utilizadores lhes tiverem dado consentimento. Regra geral, o objetivo destas empresas terceiras é criar marketing direcionado — campanhas baseadas nos assuntos das conversas que as pessoas têm online. Contudo, para garantir que não tem apps com este tipo de acesso — sobre o qual não se lembra de ter dado consentimento —, a Google lembrou que é possível ver [aqui](#) quem tem acesso e a quê. Porque a “reserva da intimidade da vida privada” deve ser respeitada. Durante a vida ou depois da morte.

[Voltar ao índice](#)

## PARTILHE



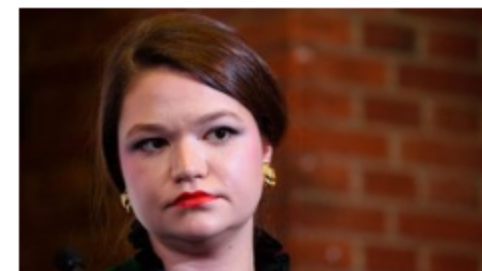
## COMENTE

2 Comente e partilhe as suas ideias

## SUGIRA

Proponha uma correção, sugira uma pista: [mmachado@observador.pt](mailto:mmachado@observador.pt)

## RECOMENDAMOS



CONFERÊNCIAS

**Ex-diretora da Cambridge Analytica vem a Portugal**

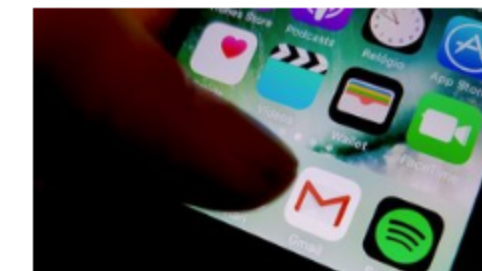
16/7/2018, 16:19



TECNOLOGIA

**Microsoft: mais leis para reconhecimento facial**

13/7/2018, 19:12



GOOGLE

**Programadores lêem os emails que troca no Gmail**

4/7/2018, 17:24



FACEBOOK

**F8: Como o Facebook quer recuperar da Analytica**

3/5/2018, 10:44



FACEBOOK

**Eurodeputados querem Zuckerberg no Parlamento**

18/4/2018, 21:01

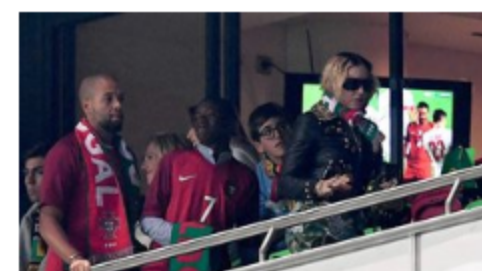


INTERNET

**Deco Proteste reuniu-se com Facebook**

11/4/2018, 14:25

## POPULARES



MADONNA

**O que ganha Portugal com Madonna (e vice-versa)? /premium**

15/8/2018, 22:50 [18](#)



IRAQUE

**Iraque. Estes monges resistiram ao Estado Islâmico /premium**

15/8/2018, 19:47 [447](#)



MADONNA

**Seis vezes em que Madonna mudou o mundo /premium**

15/8/2018, 15:42 [152](#)



SAÚDE

**Glifosato causou cancro ao jardineiro americano? /premium**

15/8/2018, 14:59 [151](#) [16](#)



TURISMO

**"Help!" O 112 anda a atender bem os turistas? /premium**

15/8/2018, 13:34 [123](#)

## ÚLTIMAS



VODAFONE PAREDES DE COURA

**Marlon apaixonou-se, os Linda Martini controlaram**

Há 28 minutos



GOVERNO

**Governo acaba com reforma obrigatória aos 70 anos**

Há 19 minutos

PORTUGAL 2020

**Quando queremos, somos os melhores /premium**

Paulo Tunhas

Há uma hora

Sobre a proposição metafísica de Marcelo relativa à natureza dos portugueses: se, quando queremos, somos os melhores dos melhores, porque é que, tantas vezes, o queremos tão pouco?





BENFICA

### PJ investiga transferências do Benfica para o Aves

Há 38 minutos



TAP

### TAP acaba com viagens à borla para governantes

Há uma hora



JOSÉ MOURINHO

### Documentário do Manchester City goza com Mourinho

Há 23 minutos

## OBSERVADOR

Rua Luz Soriano 67, 2ºE  
1200-246 Lisboa  
©2018

### Seguir

- Facebook
- Twitter
- LinkedIn
- Instagram
- Youtube
- Google+
- RSS

### Sobre

- Política de Privacidade e Cookies
- Termos e Condições
- Como anunciar
- Ficha Técnica
- Estatuto Editorial
- Regras da Comunidade
- Contactos
- Ajuda

### Descobrir

- Autores
- Tópicos
- Newsletters
- Eventos
- Conversas
- Podcasts
- MAGG

### Instale a nossa App

Disponível gratuitamente para iPhone, iPad, Apple Watch e Android

