Despite all the noise, does the DPA in reality provide an effective privacy remedy or has its value been exaggerated? When does the DPA give claimants the edge?

Hugh Tomlinson QC and Aidan Wills – Matrix Chambers

INTRODUCTION

1. Media and information lawyers have had to cope with a proliferation of causes of action and the increasing blurring of the boundaries between them. Twenty years ago we had only defamation and breach of confidence. Now, under the influence of Article 8 of the European Convention on Human Rights we have a family of "Article 8 torts" which overlap and shade into each other: harassment, misuse of private information and breach of data protection rights have come on to the scene.

2. The broad categories of interests protected by each cause of action are well known:
   - Defamation protects the right to reputation;
   - Breach of confidence protects confidential information;
   - Harassment protects physical and psychological integrity;
   - Misuse of private information protects the right to private information;
   - Data protection law encompasses the right not to have one's personal data processed unfairly or unlawfully.

   The elements of each tort are different. The judicial remedies are also different in part. But there are no fixed boundaries – many kinds of upsetting conduct can be pursued under 3, 4 or 5 of these causes of action.

3. Data protection law is intended to protect the right to privacy enshrined in Article 8 of the European Convention on Human Rights ("the Convention") and the Data Protection Act 1998 ("DPA") has been referred to as a "privacy statute"[1]. But it protects a wider range of interests. That is why the European Charter of Fundamental Rights ("the Charter") contains both a right to "respect for private and family life" (Article 7) and a right to "protection of personal data" (Article 8).

4. The right to protection of personal data encompasses "private information" but goes much wider. "Personal data" covers any information which relates to a living individual who can be identified, directly or indirectly, from that information. There may be arguments at the margins but this plainly covers any significant information about a living person, regardless of whether or not it is publicly known or plain and obvious and notwithstanding whether or not it is true or false. Not all such information falls within the ambit of Article 8 of the Convention or, if it does, Article 8 is engaged at a very low level.

5. The processing of personal data must be conducted in accordance with the rules set out in the DPA, which transposed into UK law Directive 95/46/EC on the protection of individuals with regard to the processing of personal data ("the 1995 Directive"). From May 2018 those rules will be found in two places – the General Data Protection Regulation ("GDPR") and (what will become) the Data Protection Act 2018.

---

1 *Law Society v Kordowski* [2014] EMLR 2 at [97] per Tugendhat J.

6. In this paper we consider – from the point of view a claimant – the advantages and disadvantages of data protection remedies as compared to the torts of misuse of private information and libel. We will begin with "advantages" and then move to "disadvantages" finally looking briefly at the balance.

ADVANTAGES

Breadth of the concept of personal data

7. The "gateway" into a data protection claim is much wider than in the case of the other "information" torts. The only precondition is that claims must relate to "personal data" that is information about an identified or identifiable living individual, which is being is being "processed" in any way.

8. By contrast, in the law of privacy a claimant must establish that s/he has reasonable expectation of privacy in relation to the information concerned (as to which, see *Murray v Express Newspapers* ([2009] Ch 481 at [36]).

9. Information that is personal or even sensitive personal data for the purposes of the DPA will not necessarily attract a reasonable expectation of privacy. By way of example, in *CG v Facebook Ireland* [2017] EMLR 12 Morgan LCJ urged "considerable caution" against reading across from definition of sensitive personal data in section 2 of the DPA for the purposes of the law of privacy (at [45]).

10. Information does not cease to attract the (potential) protection of data protection law in many of the circumstances in which there is unlikely to exist or to remain a reasonable expectation of privacy. Notable examples include photographs of adults taken in public places; information as to the commission of criminal offences or other disreputable conduct; and information that is in the public domain/has been widely published.

Lack of substantive defences

11. Any publication of personal data will amount to data processing regardless of whether it is online or in hard copy (having been prepared by electronic means). Any digital photograph is personal data. If a publication is subject to the requirements of the DPA – a big "if" given the range of "exemptions" available, which we will deal with under "disadvantage" – then there are limited grounds upon which a data controller can justify or defend the data processing.

12. The processing of personal data must be "fair and lawful" (the First Data Protection Principle). Compliance with one or more of the conditions in schedule 2 to the DPA will justify processing as such – most notably consent and the legitimate interests of the data controller. (paragraph 6 of schedule 2 to the DPA). In the latter case that the condition does not apply where the processing is "unwarranted … by reason of prejudice to the rights and freedoms or legitimate interests of the data subject". This requires consideration to be given to the Convention and Charter rights of the data subject.

13. The processing of sensitive personal data is extremely difficult to justify.

Sensitive personal data[2] covers matters which are obviously private

- Physical or mental health or condition;
- Sexual life

and some which are not

- Racial or ethnic origin
- Political opinion
- Religious or similar beliefs

And then there two perhaps debatable categories

- Commission or alleged commission of any offence;
- Proceedings for any offence committed or alleged to have been committed or the sentence of any court in such proceedings.

14. The only relevant conditions for publishers seeking to justify the processing of sensitive personal data are likely to be "explicit consent" (paragraph 1 of schedule 3 to the DPA) or that the data "had been made public as a result of steps deliberately taken by the data subject" (paragraph 5 of schedule 3 to the DPA). As a result, someone who is subject to the data protection principles and who publishes sensitive personal data is going to have a hard time establishing that the publication is lawful.

15. There are similar potential advantages to someone who wishes to claim that data which have been published are false or inaccurate. The Fourth Data Protection Principle requires that "personal data shall be accurate". The threshold for what is inaccurate is very low: data are inaccurate if they are incorrect or misleading as to *any* matter of fact (section 70(2) DPA).

16. Words alleged to be defamatory will almost always been impugnable on the grounds of inaccuracy. Processing such data (including by way of publication) will breach the DPA unless one of the exemptions applies (see below). Establishing inaccuracy is clearly easier than demonstrating that words (albeit presumptively false) bear a defamatory meaning and have caused or are likely to cause serious harm to a claimant's reputation.

17. In contrast to libel, data protection law may assist not only in relation to the publication of "false facts" but also in respect of true information or expressions of opinion. As noted above, data protection remedies can be sought on the basis that personal data are not being processed fairly and lawfully as the processing did/does not meet one of the conditions in schedule 2 to the DPA (and if the data are sensitive personal data, an additional condition in schedule 3). Where one or more of the conditions are not met and the defendant is not able to bring their data processing within one of the exemptions, it does not matter whether the personal data are true or a statement of opinion which may be entirely defensible in libel.

18. Claimants in DPA proceedings not need to prove publication, which can sometimes be difficult in libel claims. It is sufficient to show that the data controller is processing (or has processed) the claimant's personal data. This is rarely in dispute.

[2] The GDPR refers to these as "special categories of data" and has enlarged the types of data falling within this grouping to including genetic data, biometric data for the purpose of uniquely identifying a natural person, and data concerning sexual orientation (article 9).

Data protection claims can be brought in tandem with other claims

19. It is now clear that data protection claims may be brought alongside libel claims arising from the same set of facts. In *Prince Moulay Hicham Ben Abdallah Al Alaoui of Morroco v Elaph Publishing Ltd* ([2017] 4 WLR 28), Simon LJ held that there is

> "no good reason of principle why a claim under the DPA cannot be linked to a defamation claim, … In the present case Elaph contend that the article is not defamatory of the Prince. If that defence succeeds the DPA claim may found an appropriate alternative means of redress.." at [44].

20. Exactly the same reasoning must apply to claims for misuse of private information or harassment. The publication of private information or the repeated publication of "harassing material" will also be a potential breach of the DPA and there is nothing to prevent the claims being joined. In practice, this is now regularly done.

The DPA enables claimants to make "delisting" claims against search engines

21. The area in which data protection law offers the most significant advantages for claimants is in respect of search engines. As the law currently stands, for the purposes of misuse of private information and libel, the operators of search engines are not regarded as "publishers" at common law regardless of whether or not they have notice that unlawful material is being generated/made available through search results (*Metropolitan International Schools Ltd v Designtechnica Corporation and others* [2011] 1 WLR 1743).

22. Similarly, search engine operators are not "hosts" within the meaning of the E-Commerce Directive 2000 and the E-Commerce Regulations 2002. This is of significance because hosts may be liable for defamatory or privacy-violating information posted by their users if they have actual or constructive knowledge of the impugned information and fail to remove or disable access expeditiously.

23. Data protection law offers a tailor-made solution for claims against search engines. In *Google Spain SL & another v Agencia Espanola de Protecion de Datos & Costeja* [2014] QB 1022 the CJEU recognised a right to have search results delisted (the so-called right to be forgotten). A data subject may require a search engine operator to remove search results generated by searches including her/his name, where those search results are "inadequate, inaccurate, no longer relevant, or excessive". There is no requirement for the data subject to show that s/he is being caused any prejudice by the generation of the search results. This right is not absolute; it is balanced against the public's right to have access to information on issues of public interest.

24. It is possible for a data subject to get search results removed even in circumstances in which no cause of action would lie against the primary publisher whose material appears in the results. The delisting or de-indexing of search results does not, however, prevent internet users from accessing a publication on the primary publisher's website (if they know the URL) or on other search engines.

25. An expanded "right to erasure" has been codified in the GDPR (article 17). This comes into force in May 2018.

Broader remedies under the DPA

26. Under section 10 of the DPA a data subject can require a data controller to cease (or not to begin) processing her personal data where it is causing her substantial damage or distress which is unwarranted. It is not necessary for the data subject to show that the data is being processed unlawfully under the DPA. A court can order the data controller to comply with a section 10 notice.

27. Under section 13 of the DPA claims can now be made for "general damages" (including for distress) without first needing proof of "special damage" (i.e., pecuniary loss). It is possible that a claim for damage to reputation can be made under the DPA (see *Hannon v NGN* [2014] EWHC 1580 (Ch)). The Court can also make orders similar to injunctions requiring a data controller to rectify, block, erase or rectify inaccurate personal data (section 14(1)) and/or where the data subject has suffered damage by reason of any other contravention of the DPA (section 14(4)).

28. The DPA also offers a bespoke remedy which is not available in other causes of action: a court order requiring a data controller to inform third parties to which personal data has been published of its erasure, rectification, destruction or blocking. Section 14(3) of the DPA authorises courts to make such orders in circumstances in which they have made orders under section 14(1) or where inaccurate data have already been erased, destroyed, blocked or rectified. Such a remedy is tantamount to a requirement to print or communicate a correction, which would be impossible in a libel claim.

DISADVANTAGES

Claims can only be made against Data Controllers

29. Claims for misuse of private information can be made anyone who uses the private information. Claims in libel can be made against an author, editor or publisher of the words complained of. A claim under the DPA cannot be brought against anyone who processes personal data: only against the "data controller".

30. The notion of "data controllers" is central to data protection law as it determines against whom data protection remedies may be pursued. Data protection claims can only be brought against "a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed". Evidently, this is an expansive definition which almost certainly encompasses a broader range of (would be) defendants than is often thought to be the case. This is, however, subject to the domestic purposes exemption discussed below.

31. It is strongly arguable that anyone who operates, for example, a Twitter, Instagram or Pinterest account through which they publish the personal data of other people to the whole world is a data controller. They are therefore subject to the provisions of the DPA.

Claims cannot be made against individuals processing for "domestic purposes"

32. Section 36 of the DPA exempts from the data protection principles and the provisions of parts II and III of the Act, personal data processing by an individual only for the purposes of that individual's personal, family or

household affairs (including recreational purposes).

33. Under the 1995 Directive, the CJEU has interpreted this provision narrowly (e.g., C:2014:2428 *František Ryneš v Úřad pro ochranu osobních údajů* at [30] – [35]; C:2003:596 *Bodil Lindqvist* at [47]). By way of example, operating a CCTV camera on the exterior of a domestic property has been held not to fall within the exemption. Also outside the ambit of the domestic purposes exemption was the publication of personal data on a (public) website set up on a home computer for the purposes of providing information to fellow parishioners.

34. The GDPR *may* have narrowed the application of data protection law to such activities. Article 2(2)(c) provides that the GDPR does not apply to data processing by a natural person in the course of a purely personal or household activity (which is same wording as in the 1995 Directive). Recital 18 to the GDPR provides a partial definition of this term, noting that "[p]ersonal or household activities could include correspondence and the holding of addresses, or social networking and online activity undertaken within the context of such activities", provided that the processing has "no connection to a professional or commercial activity". It remains to be seen whether or not this will serve to broaden the domestic purposes exemption and whether it would apply to publications made to the public at large through social media.

Partial exemptions for journalistic, literary and artistic data processing

35. Section 32 of the DPA provides an exemption from most of the statutory provisions which apply to the processing of personal data if the data is being processed "only for the special purposes"; that is, only for journalistic, artistic or literary purposes, and

> "(a) the processing is undertaken with a view to the publication by any person of any journalistic, literary or artistic material;
> (b) the data controller reasonably believes that, having regard in particular to the special importance of the public interest in freedom of expression, publication would be in the public interest; and
> (c) the data controller reasonably believes that, in all the circumstances, compliance with that provision is incompatible with the special purposes (s.32(1))".

36. "Journalism" is defined expansively under EU (and Convention) law. In the *Satamedia case* (C:2008:727) at [61], the CJEU found that the reference to journalism in the 1995 Directive should be interpreted broadly and covered the disclosure to the public of information, opinions or ideas by any means. This means that, in principle, anyone e.g., blogging or tweeting as a "citizen journalist" could rely on the section 32 exemption. Domestically, Tugendhat J has observed that journalism entails the "communication of information or ideas to the public at large" (*Law Society v Kordowski* [2011] EWHC 3185 (QB) at [99]).

37. Literary and artistic purposes are not defined in the DPA or the 1995 Directive. However, such purposes are likely to be regarded as very wide ranging. By way of analogy, section 3 of the Copyright, Designs and Patents Act 1988 defines "literary work" as encompassing any work "which is written, spoken or sung, and accordingly includes … a table or compilation … a computer program…preparatory design material for a computer program…a database".

38. Section 32 contains four conditions which must be satisfied before the exemption is available:
(1) the data is processed *only* for journalism, art or literature,
(2) with a view to publication of some material,
(3) with a reasonable belief that publication is in the public interest, and
(4) with a reasonable belief that compliance is incompatible with journalism.
These will be considered in turn, with a focus on journalism as a special purpose.

39. **First condition: "only for the special purpose(s)"**. This is a question of fact but it is likely that a media organisation would be able to satisfy this requirement in any case where information is being collected, stored and edited for the purposes of publishing articles. It is less clear that this criterion would be met if such data are also being processed for the purposes of, for example, advertising.

40. **Second condition: "with a view to publication"**. The data controller must show that the personal data were/are processed with a view to the publication of <u>any</u> journalistic, artistic and literary material. In other words, what has to be contemplated is not the publication of the data in question but the publication of <u>some</u> journalistic, artistic or literary material. This requirement is unlikely to be difficult to satisfy.

41. As the ICO says in its publication *Data Protection and Journalism: a guide for the media* ("the ICO Guide"):

> "this means that the exemption can potentially cover any information collected, created or retained as part of a journalist's day-today activities, both before and after publication. However, the exemption cannot apply to anything that is not an integral part of the newsgathering and editorial process. For example, information created in response to a complaint about a particular story after publication is unlikely to be processed with a view to publication*" (p.30).*

It is well established that the exemption applies both before and after publication (see *Campbell v MGN* [2003] QB 633).

42. **Third condition: "reasonable belief in public interest".** This has two limbs: public interest and reasonable belief.

43. On the *first limb*, the statute appears to provide two pieces of guidance as to the meaning of "public interest". The first, which is more apparent than real, is the reference in section 32(1)(b) to "the special importance of the public interest in freedom of expression". These words cannot be read as "privileging" freedom of expression over the privacy rights or data protection rights of data subjects. It is well established that neither the right to freedom of expression under Article 10 of the Convention, nor the right to privacy under Article 8 has, as such, precedence over the other (see *Re S (a child)* [2015] 1 AC 593 at [17]). In other words, this provision must be read as a "reminder" that Article 10 rights must be put in the balance – but not as an instruction to give them special, much less predominant, weight.

44. Second, section 32(3) refers to any code of practice designated for the purposes of the section. The Secretary of State has "designated" a number of Codes – in particular, the Ofcom Broadcasting Code, the BBC Producers Guidelines and the Press Complaints Commission Code (although, strictly speaking, this no longer exists). Common to these codes is a relatively narrow

view of the public interest. For example, the Ofcom Broadcasting Code provides that:

> "Examples of public interest would include revealing or detecting crime, protecting public health or safety, exposing misleading claims made by individuals or organisations or disclosing incompetence that affects the public"*(*p.42).

This strict view of "public interest" would be consistent with the approach to balancing privacy and expression rights in Strasbourg and under the tort of misuse of private information and is consistent with Article 9 of the 1995 Directive.

45. In short, the provision contemplates a "public interest" justification for processing of a similar type to that required to justify the publication of private or confidential information: a belief that the public will be interested in the story or that publication of stories of that type is necessary for the economic viability of the publisher will not be enough.

46. The *second limb* of this condition is the "reasonable belief" of the data controller that publication would be in the public interest. This connotes an objective assessment of the subjective views of the data controller as to the public interest in the publication of the personal data concerned. With regard to data controllers that are organisations (as opposed to individuals) there is some uncertainty as to who must hold the reasonable belief in order for this test to be met. It is likely to be the person within the organisation responsible for determining the purposes for which the organisation processes personal data.

47. This exemption can only apply insofar as it is "necessary" to reconcile privacy and freedom of expression. The test must therefore be a strict one: the facts as they are reasonably believed to be at the time of processing must be such that a reasonable data controller would believe that publication would be in the public interest. Any lower hurdle would not meet the necessity test.

48. Any data controller who seeks to rely on a special purposes exemption must be in a position to show that specific consideration was given to the processing in question and to the public interest. "After the event" justification will not be enough as the mandatory conditions for the exemption will not have been satisfied at the time the data was processed.

49. **Fourth Condition: "Compliance would be 'incompatible' with journalism"**. The data controller must reasonably believe that, in relation to each of the relevant provisions of the DPA, compliance with that provision is "incompatible with the special purposes".

50. The ICO's Guide suggests that this means that the data controller must reasonably believe that it is "impossible both to comply with a particular provision" and fulfil the journalistic purpose (p.37). When considering "incompatibility", the data controller cannot rely on a blanket policy but must give specific consideration to the factual position in each case.

51. In some cases the incompatibility will be obvious: for example, allowing the subjects of ongoing public interest journalistic research to make subject access requests would make that kind of journalism impossible. The same applies to seeking the consent of the data subject (one route to compliance with the First Data Protection Principle) in the context of an investigation into her/his conduct. It is, however, less clear that other provisions of the DPA should not

apply in such cases: if the publication is in the public interest then it is likely that the condition in Schedule 2, para 6 can be satisfied – namely that the processing is necessary for the purposes of legitimate interests pursued by the data controller and the processing is not "unwarranted".

52. In the case of other kinds of journalism it is may be difficult to see why compliance the provisions of the DPA makes journalism impossible. There seems to be no inherent incompatibility between, for example, subject access requests and "entertainment" journalism. Furthermore, the data of celebrities can be processed fairly and lawfully without making journalism "impossible".

53. The ICO Guide suggests (p.37) that the incompatibility condition may be satisfied where compliance is not practical. This is not, however, a qualification to be found in the DPA or the 1995 Directive. In general, the DPA does qualify duties owed to data subjects on the basis of considerations of "practicality" and there is no obvious reason why this requirement should be read into section 32(1)(c). The criterion – based on Article 9 of the 1995 Directive – must be "necessity" not practicality. In other words, is the exemption from the provisions of the DPA necessary to allow the journalist to fulfil the purposes of journalism? If it is not necessary then the provisions should be complied with.

54. While the special purposes exemption is capable of being relied by a wide range of data controllers in many data processing contexts, the conditions that must be satisfied are more exacting than is often thought to be the case.

No interim remedies available

55. Section 32 of the DPA contains a provision designed to prevent "pre-publication" claims where unpublished journalistic, literary or artistic material is involved.

56. The relevant parts of section 32 provide as follows:

> "(4) Where at any time ("the relevant time") in any proceedings against a data controller under section 7(9), 10(4), 12(8) or 14 or by virtue of section 13 the data controller claims, or it appears to the court, that any personal data to which the proceedings relate are being processed—
>
> (a) only for the special purposes, and
>
> (b) with a view to the publication by any person of any journalistic, literary or artistic material which, at the time twenty-four hours immediately before the relevant time, had not previously been published by the data controller, the court shall stay the proceedings until either of the conditions in subsection (5) is met.
>
> (5) Those conditions are—
>
> (a) that a determination of the Commissioner under section 45 with respect to the data in question takes effect, or
>
> (b) in a case where the proceedings were stayed on the making of a claim, that the claim is withdrawn.

57. A "determination of the Commissioner" (that is, the ICO) under section 45 is a "determination in writing" that any personal data

> (a) are not being processed only for the special purposes, or
>
> (b) are not being processed with a view to the publication by any person of any journalistic, literary or artistic material which has not previously been published by the data *controller,*

In other words, the effect of section 32(4) and (5) is that, if it appears that someone is processing unpublished personal data for journalistic, artistic or literary purposes with a view to publication, the Court must stay any proceedings (with the effect that an interim injunction could not be obtained to restrain publication) unless and until the ICO decides that the data is not being processed for the purposes of journalism etc with a view to publication.

58. The ICO Guide says of section 32(4) that*:* "[i]n effect, this means that someone cannot use the DPA to prevent publication*"* (p.52). Indeed it does, but it goes further. Its effect is that no claim can be brought against any kind of publisher (not just media organisations but also "citizen journalists" and anyone else who could bring themselves within the very broad ambit of the literary or artistic special purposes) in respect of the unlawful processing of any unpublished personal data which the publisher intends to publish in the future.

59. It is important to note that the "stay" does not depend on the other conditions in section 32 being fulfilled – as long as the publisher is processing the personal data with a view to publication there is no need for the publisher to demonstrate reasonable belief that the publication would be in the public interest (section 32(1)(b)) or that compliance with the provisions of the DPA would be incompatible with the special purposes (section 32(1)(c)).

60. Having regard to the breadth of the special purposes (see above), the consequence of these provisions is that it is extremely difficult to obtain a pre-publication injunction under data protection law.

61. This scheme was challenged in *Stunt v Associated Newspapers* ([2017] 1 WLR 3985). Popplewell J surprisingly held that this provision was compatible with EU Law. The case is subject to appeal.

BALANCE SHEET

62. As compared to privacy, data protection's primary advantage is the lack of any requirement to establish that there is a reasonable expectation of privacy in relation to the information concerned. Its main advantages over libel are that false information is actionable at a much lower threshold and a publication may be give rise to a successful claim even if the personal data are true or an expression of opinion.

63. Data protection law provides a remedy for those whose personal data is published in circumstances in which there cannot be any reasonable belief in public interest: "entertainment journalism". For example, it provides a clear remedy in relation to "paparazzi photographs" of celebrities without any need to get into subtle arguments about whether there is a "reasonable expectation of privacy". Photographs are personal data – and possibly sensitive personal data – and the processing is highly unlikely to be fair or lawful.

64. Through the right to be forgotten / delisting, data protection law provides an increasingly valuable remedy for people whose main concern is to prevent material relating to them being made available through search engine results. In many cases, this may be as valuable (and often easier to obtain) than remedies against primary publishers.

65. Data protection law does not provide an effective "pre-publication" remedy for any kind of privacy or accuracy complaint if the *Stunt* decision stands (and the

provisions equivalent to section 32(4) and (5)) remain the in the Data Protection Bill.

66. While our focus has been on legal claims, data protection law also provides an "administrative" route through which data subjects can (under section 42 of the DPA) call upon the Information Commissioner to assess whether or not it is likely that their personal data is being processed in compliance with the Act. This may be give rise to an enforcement notice under section 40 requiring the data controller to comply with particular provisions. Referring a matter to the ICO has the advantage that it is a free and largely confidential process – enforcement decisions are published in anonymised form – which may be of value for some claimants. This process may, however, be slow and the ICO does not have the power to award any compensation to data subjects.

67. Overall, data protection law provides an increasingly useful and flexible set of tools for claimants seeking the removal/blocking or correction of (and compensation for) information already published about them. These remedies can legitimately be deployed alongside claims for misuse of private information, breach of confidence, harassment and/or libel.

Hugh Tomlinson QC

Aidan Wills

Matrix Chambers

20 November 2017