Chapter 7

Theoretical foundations of data protection in light of comparative conclusions and South African law of delict

Contents

1 INTRODUCTION

From the comparative analysis, it is evident that data protection entails the legal protection of a person[1] (called the data subject) with regard to the processing of data concerning himself or herself by another person or institution.[2] The aim of this chapter is to analyse the private law foundations[3] of the legal

1 Although the primary concern is data relating to an identified or identifiable natural person (see ch 6 par 2.5.3), data on juristic persons can also be included (see par 2.5.2 below).

2 Neethling *Persoonlikheidsreg* 321. See also Gellman 1994 *Gov Inf Q* 245, 246 according to whom data protection "focusses attention more precisely on laws, policies, and practices that affect the collection, maintenance, and use of personal information about individuals". See further ch 1 par 1.6.

3 Data protection also has a basis in constitutional law and criminal law can play a role in the enforcement of data protection obligations. Although attention is briefly paid to the way in which these fields are (continued...)

protection of the data subject in South African law from a theoretical viewpoint and to establish to what extent, if any, the data protection principles expounded in the previous chapter are reflected in our law.[4] This will make it possible to establish which of the data protection principles are not given (sufficient) effect to in South African common law and thus what lacunae exist which should be rectified.

2 PRIVATE LAW BASIS FOR PROTECTION

2.1 Interests involved

The processing of information or data on a person by a data controller primarily threatens the privacy and identity of the data subject.[5] Privacy and identity are both personality interests. A personality interest is a non-patrimonial interest that cannot exist separately from the individual.[6] Personality rights are characterised by the fact that they cannot be transferred to others, cannot be inherited, are incapable of being relinquished, cannot be attached and that they come into existence with the birth and are terminated by the death of a human being[7] (or in the case of a juristic person, when such person comes into existence or ceases to exist).[8]

Different personality interests have been identified, such as the body, physical liberty, good name,

3(...continued)
involved in data protection in the different countries studied, a detailed investigation of the theoretical foundations of data protection in constitutional and criminal law falls outside the scope of this thesis.

4 The next chapter explores the question whether the protection of the data subject that is theoretically possible in our law has been realised in positive law; in other words, to what extend data protection is in fact implemented under South African law.

5 Why this is so, will be explained in par 2.3.2.1 below. A person's good name and dignity may also be involved (see Neethling *Persoonlikheidsreg* 326 fn 46).

6 See Neethling *Persoonlikheidsreg* 14 and authority cited there.

7 Joubert *Grondslae* 124 *et seq*; Neethling *Persoonlikheidsreg* 17.

8 Neethling *Persoonlikheidsreg* 17 fn 139.

dignity, feelings, privacy and identity.[9] These personality interests are refinements of the broader triad of the Roman law, namely *corpus, fama* and *dignitas.*[10] Privacy and identity are considered to be part of the *dignitas* concept, which is a collective term for all personality aspects apart from *fama* (good name) and *corpus* (physical integrity).[11] The infringement of a personality interest leads to non-patrimonial loss.[12]

Other interests of a patrimonial nature may also be at risk when data processing takes place. For example, a person's creditworthiness can be infringed if incorrect information concerning his or her creditworthiness is processed.[13] Where these other interests are relevant they will merely be referred to in passing, since the main focus of this thesis is on the personality interests involved.[14]

---

9 For a detailed discussion of these personality interests, see Neethling *Persoonlikheidsreg* 31–47. But see Burchell *Delict* 189 *et seq* and *Personality rights* 327 *et seq* who argues for a broad interpretation of dignity to include personality interests such as reputation and privacy, as well as the individual's right to personal autonomy. He argues that it is important that the courts should adopt a "broad, human rights oriented interpretation to the civil-law concept of dignity" (Burchell *Delict* 189).

10 See Neethling *Persoonlikheidsreg* 53; Van der Merwe & Olivier *Onregmatige daad* 10; Van der Walt & Midgley *Delict* 14–15 (par 10); *Universiteit van Pretoria v Tommie Meyer Films (Edms) Bpk* 1977 4 SA 376 (T) 384.

11 *Bernstein v Bester NO* 1996 (2) SA 751 (CC) 789; *Jansen van Vuuren v Kruger* 1993 4 SA 842 (A) 849; Neethling *Persoonlikheidsreg* 231.

12 For more on this, see par 2.3.5 below.

13 Klopper *Kredietwaardigheid* 15 244 defines creditworthiness as the characteristic, attribute or ability of a person (including a juristic person) to invoke confidence on the part of a creditor in his or her willingness and ability to pay his or hers debts in future. Such a characteristic is obtained by the person's previous active use of credit. Because creditworthiness has a patrimonial character it cannot be classified as a personality interest (Klopper *Kredietwaardigheid* 249; Neethling *Persoonlikheidsreg* 21). A discussion of the precise nature of creditworthiness falls outside the scope of this thesis (in this regard see Klopper *Kredietwaardigheid*). Klopper 249 classifies creditworthiness as a separate immaterial property right, whereas Neethling *Persoonlikheidsreg* 22 describes it as personal immaterial property. Neethling shows that creditworthiness does have some of the characteristics of personality rights, in that it cannot exist without being connected to a person and it cannot be transferred, inherited or attached (Neethling *Persoonlikheidsreg* 20; *contra* Klopper *Kredietwaardigheid* 241–243).

14 At this point, the interplay between creditworthiness on the one hand and privacy and identity on the other hand in the area of data protection should be noted. The fact that credit information is collected on a person in order to establish such person's creditworthiness creates a potential threat to the privacy and identity of the person, especially if the person has no control over the information collected. On the other hand, where data protection principles are in place, creditworthiness may also be protected in the sense that the credit information collected will be more accurate since the creditor will have control over his or her credit

(continued...)

2.2 Delictual protection

2.2.1 Traditional common law principles

In private law,[15] the individual's rights to his or her personality[16] are protected by means of the law of personality, which forms part of the law of delict. The remedies for the protection of a person's personality are therefore of a delictual nature. This means that in South African common law a person can rely on the law of delict for protection of his or her rights infringed by the processing of personal information.[17] These rights, which are recognised and protected interests in South African law, are primarily the rights to privacy and identity.[18]

In South African law, the question of delictual liability is governed by a generalising approach,[19] allowing for the recognition and protection of personality interests, such as privacy, which have only come to the

14(...continued)
information (see Klopper *Kredietwaardigheid* 91).

15 Personality rights are also directly or indirectly protected by criminal law (eg sanctions against crimes such as murder, culpable homicide, assault, rape, *crimen iniuria* (see Jansen 2002 (Apr) *De Rebus* 29–31), criminal defamation and kidnapping (see further Snyman *Criminal law*)), administrative law and constitutional law, specifically in terms of the Bill of Rights. Ch 2 of the Constitution of 1996 recognises the right to human dignity (s 10), the right to life (s 11), the right to freedom and security of the person (s 12) and the right to privacy (s 13) as fundamental rights. According to Neethling *Persoonlikheidsreg* 20, personality rights which are enshrined in a bill of rights do not change their juridical character. They remain personality rights, but receive stronger protection in that the legislature and the executive of the state may not pass any law or take any action which infringes or unreasonably limits such rights. Since the Bill of Rights also has horizontal application – ie between individuals – personality protection between individuals is also enhanced. See further par 2.2.2.

16 The expression "rights to personality" was used in South African case law as early as 1908, when Innes CJ in *R v Umfaan* 1908 TS 62 68 referred to "those real rights, those rights *in rem*, related to personality, which every free man is entitled to enjoy." See further Neethling *Persoonlikheidsreg* 3 *et seq*.

17 As a general rule the laws of South Africa apply to all persons in the country, including foreign citizens (Dean "SA" 381).

18 See above par 2.3.2.1.

19 This means that general principles or requirements regulate delictual liability. The opposite of this is a casuistic approach (eg of English and Roman law) where a wrongdoer will only be held liable if his or her conduct satisfies the requirements of a specific tort (ie delict) (see Neethling *Persoonlikheidsreg* 4; Van der Walt & Midgley *Delict* 18–19 (par 18); Alheit *Expert systems* 140).

fore in modern times.[20] The elements of a delict are evident from the generally accepted definition thereof: A delict is the wrongful, culpable conduct of a person causing harm to another.[21] In other words, the requirements are an act, wrongfulness, fault, causation and damage.[22]

2.2.2 Influence of Constitution on law of delict

Apart from the traditional common law principles it is important to note that the Constitution,[23] especially the Bill of Rights,[24] may have a profound influence on the delictual protection of personal data. In *Carmichele v Minister of Safety and Security (Centre for Applied Legal Studies Intervening)*[25] the Constitutional Court put it unequivocally that, in the light of section 39(2) of the Constitution,[26] there is a general duty on the courts to develop the common law with reference to the spirit, purport and object of the Bill of Rights. Neethling[27] emphasises, however, that it is important to keep in mind that this general duty does not give judges *carte blanche* to change the common law arbitrarily. The court stressed that the most important force behind legal reform was still the legislator and not the judiciary. An investigation into changing existing common law should comprise a two-fold process. Firstly, it would have to be established whether existing common law requires revision in the light of the constitutional objectives, that is, whether the development of the common law is necessary,

20 Neethling, Potgieter & Visser *Delict* 5; Alheit *Expert systems* 141.

21 *Perlman v Zoutendyk* 1934 CPD 151, 155; Boberg *Delict* 24–25; Neethling, Potgieter & Visser *Delict* 4; Van Aswegen *Sameloop* 135; Van der Merwe & Olivier *Onregmatige daad* 24; Van der Walt & Midgley *Delict* 2–3 (par 2).

22 See par 2.3 for a discussion of the elements.

23 Constitution of the Republic of South Africa Act 108 of 1996. Cited as Act 108 of 1996 and referred to as "the Constitution of 1996" or "the 1996 Constitution", or "the Constitution".

24 Ch 2 of Act 108 of 1996.

25 2001 4 SA 938 (CC). For discussions hereon, see Leinius & Midgley 2002 *SALJ* 17; Pieterse 2002 *SALJ* 27; Neethling & Potgieter 2002 *THRHR* 265.

26 Requiring that "when interpreting any legislation, and when developing the common law or customary law, every court, tribunal or forum must promote the spirit, purport and objects of the Bill of Rights".

27 See further Neethling 2002 *THRHR* 574, 586.

and if so, secondly, how such development should take place.[28]

The direct application of the Bill of Rights[29] has resulted in the strengthening of entrenched rights, largely through the constitutional imperative which obliges the state to respect, protect, promote and fulfil the rights in the Bill of Rights.[30] In the present context, the right to privacy is important. The Bill of Rights expressly recognises the right to privacy as a fundamental human right in section 14. Identity is not recognised *eo nomine* but, like the right to a good name (*fama*) which is also not mentioned explicitly, it can be considered to be protected under the right to dignity, which is mentioned explicitly in section 10.[31] The concept of human dignity in the Constitution can thus be compared with the wide *dignitas* concept of common law.[32] A strong case may be made that the entrenchment of the right to privacy (and identity) is an indication of the state's legal duty to take reasonable steps to prevent a person's privacy from being infringed by third parties.[33]

The rights that are expressly constitutionally entrenched obviously also play an important role in the

28 See further Neethling 2002 *THRHR* 574, 586–587.

29 The application of the Constitution to the common law may be vertical (in so far as it binds the state and its organs – Constitution, s 8(1)), as well as horizontal (in so far as it binds natural and juristic persons – Constitution, s 8(2)), and may be either direct or indirect (Neethling *Persoonlikheidsreg* 92–93; Neethling, Potgieter & Visser *Delict* 19–23). Vertically, its direct operation means that the state is obliged to respect the fundamental rights applicable to the field of the law of delict in so far as the relevant rights are not limited in terms of the limitation clause of the Bill of Rights (Constitution, s 36(1)). Horizontally, its direct operation means that, by means of the application (and where necessary development) of the common law, the courts must give effect to the fundamental rights relevant to or related to the field of the law of delict to the extent to which legislation does not do so (Constitution, s 8(3)). In contrast, the indirect operation of the Bill of Rights means that all private law principles and rules – including those that govern the law of delict – are subject to and must thus given content in the light of the basic values of the Bill of Rights. In this regard, the courts must promote the spirit, purport and objects of the Bill of Rights in the development of the common law (Constitution, s 39(2)).

30 Act 108 of 1996 ss 7(2)) and 205(3). See Neethling 2002 *THRHR* 574, 586.

31 See further par 2.3.2.1.

32 See par 2.1. Also see Neethling *Persoonlikheidsreg* 96. According to *Gardener v Whitaker* 1995 2 SA 672 (E) 690 "the right to respect for and protection of human dignity in s 10 of the Constitution ... seems to encompass something broader than the Roman-Dutch concept of *dignitas*...". See also Burchell *Personality rights* 328 *et seq*; *Delict* 14. But see Van Aswegen 1995 *SAJHR* 50, 63–64 who argues that Burchell's concept of dignity, that embraces all fundamental rights, is too wide.

33 See also Van der Merwe *Computers and the law* 131.

indirect application of the Bill of Rights, as happened in the *Carmichele* case. Indirect application is particularly relevant in the case of "open-ended" or pliable principles of delict, namely the *boni mores* test for wrongfulness, the accountability test for legal causation and the reasonable-person test for negligence, where policy considerations and factors such as reasonableness, fairness and justice may play an important role.[34] Therefore, the basic values which underpin the Bill of Rights could be implemented to good effect as important policy considerations in the determination of wrongfulness, legal causation and negligence. This approach is already followed in case law and was expressly applied in *Carmichele*. In fact, the court suggested that the application of the Bill of Rights to the law of delict *in casu* could lead to an emphasis on the objective nature of wrongfulness as a delictual element, and that this element would be defined more clearly and broadly. The court also suggested that fault and legal causation should play a more important role in limiting liability. A proper application of these delictual elements should also allay the fear of the unbridled extension of liability. According to the Constitutional Court, the process of a re-appraisal of the content of wrongfulness, in particular, may result in existing principles and norms being either replaced or expanded and enriched by the value system embodied in the Constitution. Since the legislator – and not the courts – is the most important force in developing the common law in this respect, the process of replacing or enriching the existing norms must nevertheless be approached with caution.[35]

The Constitutional Court's approach in *Carmichele* to the application of the Bill of Rights to the law of delict provides the basis for a healthy interaction between *de lege lata* principles of the law of delict and the *de lege ferenda* role that the spirit, purport and object of the Bill of Rights should play in this field of law.[36]

34 See par 2.3 below.

35 Therefore, it is suggested that in the exercise of this process, the general principles which have already crystallised in respect of the reasonableness or *boni mores* criterion (legal convictions of the community) for delictual wrongfulness may still be regarded as a *prima facie* indication of the reasonableness or not of an act (see Neethling, Potgieter & Visser *Delict* 22; Neethling *Persoonlikheidsreg* 69, 95 fn 389).

36 See Neethling & Potgieter 2002 *THRHR* 265, 272.

2.3 Delictual requirements

2.3.1 Act

Only voluntary human conduct qualifies as an act for the purposes of the law of delict.[37]

Therefore the conduct must firstly be that of a human. A juristic person acts through its organs (director, official or servant) and may thus be held delictually liable for such actions.[38] The relevant conduct is an act which is performed by a human being, but which is attributed to a juristic person on account of the human's connection with that person. Neethling, Potgieter and Visser suggest the following guideline to determine whether a human act may be attributed to a juristic person (legal corporations): "An act performed by or at the command or with the permission of a director, official or servant of the legal corporation in the exercise of his duties or functions in advancing or attempting to advance the interests of the legal corporation, is deemed to have been performed by such corporation."[39] Data controllers, who more often than not are legal corporations or juristic persons, can therefore also be held liable for the wrongful processing of data. Note also that the conduct of a person who is not the data controller or data processor, but who assists, aids or abets in wrongful data processing, also qualifies as conduct and in principle such a person is also liable in delict.[40]

Secondly, the conduct must be voluntary. Voluntary means that the conduct must have been susceptible

37 Neethling, Potgieter & Visser *Delict* 27; Van der Merwe & Olivier *Onregmatige daad* 25. The conduct must of course be that of the defendant, or of an employee, for whose conduct the employer is vicariously liable. In the case of vicarious liability, someone is held liable for the damage caused by another and vicariously liability exists where there is a particular relationship between two persons, such as employer-employee, principal-agent or motor car owner-motor car driver (see Neethling, Potgieter & Visser *Delict* 373; Van der Merwe & Olivier *Onregmatige daad* 1 24; Van der Walt & Midgley *Delict* 25 (par 24)).

38 Neethling, Potgieter & Visser *Delict* 27–28; Van der Walt & Midgley *Delict* 51; Van Heerden & Neethling *Unlawful competition* 66; Van der Merwe *Computers and the law* 152.

39 Neethling, Potgieter & Visser *Delict* 28 fn 6. See also Alheit *Expert systems* 146.

40 Compare *McKenzie v Van der Merwe* 1917 AD 41 51; Van Heerden & Neethling *Unlawful competition* 67.

to human control; it need not be willed or desired.[41] If the actor is capable of making a decision about the conduct and is capable of preventing the prohibited result, the conduct is voluntary.[42]

From the comparative research, it is apparent that the act which is relevant in the area of data protection is any conduct that can be considered to be "processing" of personal data. Processing of data generally includes any act (or any set of acts) performed in relation to personal data, such as the collection,[43] recording, collation or sorting, storage, updating, modification, retrieval, consultation, use, disclosure and dissemination by means of transmission, distribution or making available in any other form, sharing, merging, linking together, alignment or combination, blocking, as well as screening, deletion or destruction of data.[44] In short, it includes any operation performed upon personal data.[45]

The fact that these types of conduct (in short, data processing) are often performed automatically by means of a computer does not result in the conduct not meeting the definition of an act as voluntary human conduct, because the computer is merely an instrument in the hands of humans.[46]

41 Neethling, Potgieter & Visser *Delict* 28; Van der Merwe & Olivier *Onregmatige daad* 25.

42 Alheit *Expert systems* 146.

43 It is important to note that from the moment the personal data are collected, data protection principles should be applicable (Holvast 1998 (1) *Priv & Inf* 4, 5).

44 WBP 1(b); Dir 95/46/EC a 2(b). Also see DP Act of 1998 s 1(1); Convention 108/1981 a 2(c); ch 1 par 1.7.2.

45 DPR *Data Protection Act 1998* 6; Carey *Data Protection Act 1998* 9; Pounder & Kosten 1995 (21) *Data Protection News* 7. Also see ch 4 par 4.3.3.1 and ch 5 par 4.3.3.1. As will be explained under the heading of wrongfulness (par 2.3.2 below), in terms of the law of delict, data processing will in principle lead to an action for damages or an interdict if it results in personal information being collected or made known to outsiders (that is, by an act of intrusion or an act of disclosure) or if it results in personal information being incorrectly recorded or falsified. It will become clear that the collection of data without a legitimate private or public interest is in itself a wrongful act of intrusion. The mere collection of sensitive, outdated or irrelevant data, or data collected by means of a wrongful act of intrusion, should in principle also be wrongful. See further par 2.3.2 below.

46 This is analogous to where a person uses an animal to commit a delict (see eg *Jooste v Minister of Police* 1975 1 SA 349 (E) and *Chetty v Minister of Police* 1976 2 SA 450 (N)). See further Neethling, Potgieter & Visser *Delict* 27. Alheit *Expert systems* 146 explains that an expert (computer) system can also be used as an instrument to commit a delict.

An act may take the form of either a commission or an omission.[47] Therefore, not only a *commissio*, but also an *omissio* may qualify as data processing. If the controller, for example, fails to take steps to guard against unauthorised access to the personal information and outsiders gain access to such records, the controller has acted by means of an omission.[48]

However, conduct can only result in liability if it wrongfully caused harm or prejudice to another.[49]

2.3.2 Wrongfulness

Wrongfulness is determined by a juridical value judgment on an act in the light of the harmful result caused (or potentially caused in the case of the interdict) thereby.[50] An act which is, judged according to the relevant norms of the law of delict, objectively unreasonable is wrongful and thus in principle actionable.[51] The determination of wrongfulness entails a dual investigation. First, it must be determined that a legally recognised interest has in fact been infringed, in other words the conduct must have resulted in harm for the person – in our case, in the form of infringement of the personality. Secondly, the prejudice must have occurred in a legally reprehensible or unreasonable manner, in other words, violation of a legal norm must be present.[52]

47 Boberg *Delict* 210; Neethling, Potgieter & Visser *Delict* 27 32–34; Van der Merwe & Olivier *Onregmatige daad* 29 *et seq*.

48 See also Faul *Bankgeheim* 323.

49 See *Thomas v BMW South Africa (Pty) Ltd* 1996 2 SA 106 (C) 120.

50 Knobel *Trade secret* 237. Boberg *Delict* 31 points out that wrongfulness is not simply an attribute of defendant's conduct, but is a function of that conduct together with its consequences for the plaintiff. On wrongfulness in general, see Boberg *Delict* 30 *et seq*; Burchell *Delict* 24 *et seq*; Neethling, Potgieter & Visser *Delict* 35 *et seq*.

51 Burchell *Delict* 38; Knobel *Trade secret* 237; Neethling, Potgieter & Visser *Delict* 35 *et seq*; Van der Walt & Midgley *Delict* 54 (par 55).

52 Neethling, Potgieter & Visser *Delict* 35; Van der Merwe & Olivier *Onregmatige daad* 29.

2.3.2.1 Factual infringement of personality interest

The processing of data can factually infringe a person's personality primarily in two ways:

- Where true personal information is processed, a person's privacy is infringed.
- Where false or misleading information is processed, the person's identity is infringed.[53]

This will be explained in detail in the following section.

a Privacy

i Definition and nature

It is generally accepted that data processing poses a threat to an individual's right to privacy,[54] but similar consensus does not exist on the precise definition of privacy. In this thesis Neethling's definition is used as the point of departure. Neethling defines privacy as "an individual condition of life characterised by exclusion from publicity. This condition includes all those personal facts which the person himself [or herself] at the relevant time determines to be excluded from the knowledge of outsiders and in respect of which he [or she] evidences a will for privacy".[55]

---

53 Neethling *Persoonlikheidsreg* 325–326.

54 See ch 1 par 1.3.

55 Neethling, Potgieter & Visser *Neethling's Law of personality* 36; Neethling *Persoonlikheidsreg* 39–40. See also Dean "SA" 382. This definition has been accepted by the South African Appellate Division (now the Supreme Court of Appeal) in *National Media Ltd v Jooste* 1996 3 SA 262 (A) 271. See also *Jooste v National Media Ltd* 1994 2 SA 634 (C) 645; *Universiteit van Pretoria v Tommie Meyer Films (Edms) Bpk* 1977 4 SA 376 (T) 384; *Bernstein v Bester NO* 1996 2 SA 751 (CC) 789; *Swanepoel v Minister van Veiligheid en Sekuriteit* 1999 4 SA 549 (T) 553 . It does not fall within the scope of this thesis to research the right to privacy and its definition in detail. Such research had been undertaken by Neethling in his thesis on the right to privacy, which entailed a comparative study of the protection of privacy in German, French, American, English and South African law (quoted as Neethling *Privaatheid*). This chapter relies to a large extent on the research done by Neethling in his thesis and his subsequent works, eg *Law of personality* and *Persoonlikheidsreg*. Also see McQuoid-Mason *Privacy* in which the law of privacy in South Africa

(continued...)

From this definition, the following remarks can be made about the nature of the privacy of natural persons:

- Privacy is an individual condition of life in terms of which a certain measure of seclusion from others is maintained.[56]

- Seclusion should not be equated with a condition of spatial or physical seclusion (such as that provided by a private residence). An individual can also exist in other conditions of seclusion, such as solitude, intimacy, anonymity or reserve.[57]

- A state of seclusion implies non-acquaintance by others with an individual or his or her personal affairs in such a state.[58]

- Privacy consists of the sum total of information or facts that relate to the individual in his or her

55(...continued)
is also examined against the background of the development of the right to privacy in other legal systems, and see further Burchell *Personality rights* 365–429. For useful compilations of essays on privacy, see Wacks *Privacy (vol I)* and Ippel et al *Privacy disputed*.

56 Joubert *Grondslae* 135; Neethling *Persoonlikheidsreg* 37; Burchell *Personality rights* 365. See also Gross 1967 *NYULR* 34, 36 who defines privacy as "the condition of human life in which acquaintance with a person or with affairs of his [or her] life which are personal to him [or her] is limited", and Holmes "Privacy: philosophical foundations and moral dilemma's" 18 who defines privacy as "[F]reedom from intrusion into areas of one's life that one has not explicitly or implicitly opened to others". Also see Parent 1983 *L & Phil* 305, 306; Laurie *Genetic information* 6.

57 According to Westin *Privacy and freedom* 7, privacy, when viewed in terms of the relation of the individual to social participation, is "the voluntary and temporary withdrawal of a person from the general society through physical or psychological means, either in a state of solitude or small-group intimacy or, when among larger groups, in a condition of anonymity or reserve." Also see Gavison 1980 *Yale LJ* 421, 428 who defines privacy as "a limitation of other's access to an individual". In her view of privacy, secrecy, anonymity and solitude are all elements of privacy. Perfect privacy exists for an individual when the individual is completely inaccessible to others, and this exits when no one has any information about the individual (the element of secrecy), when no-one pays any attention to the individual (the element of anonymity) and when no-one has physical access to the individual (the element of solitude). Also see Laurie *Genetic privacy* 6.

58 See Gross 1967 *NYULR* 34, 36.

state of withdrawal from publicity, which facts are excluded from the knowledge of outsiders.[59]

- Not all information which is protected against acquaintance by outsiders forms part of privacy, since privacy only relates to personal information, that is information concerning for example the individual's personality or personal life in his or her private home.[60]

- The individual himself or herself determines which information is private, coupled with the will or desire to keep the particular facts private. If the will to keep facts private (*privaathoudingswil*) is lacking, the individual's interest in privacy is also lacking.[61]

- The individual can decide whether certain personal facts are totally excluded from the acquaintance and knowledge of outsiders, or whether only certain persons may gain knowledge thereof.[62]

- The power of the individual to determine for himself or herself the scope of his or her interest

59 Neethling *Persoonlikheidsreg* 38. Westin *Privacy and freedom* 7 also emphasises that privacy concerns information about a person and Wacks "Privacy reconceived" 77 argues for an "information-based conception of privacy".

60 Joubert *Grondslae* 135. Information that relates to trade secrets, is eg related to patrimonial property and falls outside the personality (Joubert *Grondslae* 135; Neethling *Persoonlikheidsreg* 38). Also see Knobel *Trade secret* 218–221.

61 *National Media Ltd v Jooste* 1996 3 SA 262 (A) 271–272; Neethling *Privaatheid* 286; *Persoonlikheidsreg* 38; Nabben & Van de Luytgaarden *De ultieme vrijheid* 9 17.

62 *Persoonlikheidsreg* 38. These persons may be definite or fixed (eg in the case of confidential relationships), or indefinite but restricted (eg in the case of observation or identification of an individual in a public place). If the individual decides that an indefinite number of people may be acquainted with personal facts, the facts are the subject of general knowledge and not included in his or her sphere of privacy (Neethling *Persoonlikheidsreg* 38). Also see Westin *Privacy and freedom* 31–32; Holmes "Privacy: philosophical foundations and moral dilemma's" 20–21; *National Media Ltd v Jooste* 1996 3 SA 262 (A) 271–272.

in privacy is considered to be the essence of the individual's interest in his or her privacy.[63] [64]

It is clear that data processing endangers the individual's privacy, since, as has been said, privacy consists of the sum total of information or facts that relate to the individual. Where personal information is collected or otherwise processed, the individual's privacy must therefore be involved. It might be true that not all separate pieces of information collected about an individual are necessarily private, but the total picture presented by the record of such information is usually such that the individual involved would like to restrict others from having knowledge thereof.[65]

ii Privacy distinguished from other interests

Privacy as a personality object is often confused with other objects of the personality, such as the good name, identity, dignity, feelings, or body. It is also sometimes confused with autonomy, which concerns the free exercise of a person's will and therefore falls under the concept of legal subjectivity (that is, someone's status in the law as a person and the person's capacity to possess rights and duties).[66] If it is kept in mind that privacy as a personality interest is only infringed when someone learns of true private facts about a person against the person's will, the difference between privacy and other personality objects becomes clear.

---

63 Neethling *Persoonlikheidsreg* 40. This viewpoint was also accepted in *National Media Ltd v Jooste* 1996 3 SA 262 (A). Also see Neethling 1996 *THRHR* 528, 530 and Westin *Privacy and freedom* 7 who defines privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others".

64 As will be seen, (see par 2.3.2.2) the Constitutional Court's concept of "informational privacy" is in essence also in conformity with Neethling's definition.

65 Neethling *Persoonlikheidsreg* 326; "Databeskerming" 112; "Privaatheid en universiteite" 132 fn 33. Holmes "Privacy: philosophical foundations and moral dilemmas" 21 explains it thus: "The paradox of privacy is that knowledge of a collection of acts, each of which has been witnessed by some other people without any violation of privacy, may constitute a violation of privacy when it discloses dimensions of one's life one may prefer not be shared with just anyone." In *Department of Justice v Reporters Committee for Freedom of the Press* 489 US 749 (1989) 763–764 the US Supreme Court also found that an individual's privacy can be infringed by the disclosure of that person's "rap sheet" (criminal record), although all the information (arrests, indictments, convictions and sentences) summarised on a "rap sheet" have been previously disclosed to the public. See also fn 208.

66 Neethling *Persoonlikheidsreg* 36–38 40; 1997 *THRHR* 137, 141–142. See also Gross 1967 *NYULR* 34.

Reputation or good name: Prosser, for example, is of the opinion that the "private facts" tort of American law mainly infringes the individual's interest in his or her reputation or good name.[67] However, a person's good name is only infringed if his or her reputation, that is the esteem with which the person is held in the community, is lowered. It is not a requirement for the infringement of privacy that the private facts disclosed should be defamatory.[68]

Identity: Prosser's "false light" tort, for example, requires the publication of false information.[69] However, this involves the individual's interest in his or her identity, not privacy.[70] Privacy can only be infringed by the acquaintance with true personal facts.[71]

Dignity: It is also incorrect to state that an invasion of privacy requires that a person must have felt insulted,[72] since insult relates to a person's dignity, not privacy.[73]

Feelings: The infringement of a person's "mental repose"[74] by forcing unwanted attention upon him or her, or by otherwise disturbing the person's peaceful life (for example by pestering someone with phone calls, or by making obscene suggestions) should also not be considered to be an infringement of

---

67 See ch 2 par 2.1.2.2.

68 Neethling *Persoonlikheidsreg* 37.

69 See ch 2 par 2.1.2.3.

70 See further par b below.

71 McQuoid-Mason 2000 *Acta Juridica* 227, 231 argues that false light cases should be regarded as invasions of privacy, even though the facts published are not true, because such publication has "unjustifiably exposed the plaintiff to unwanted publicity". It is submitted that this view will blur the distinction between eg privacy, identity and good name, and will lead to the unavoidable conclusion that even defamation by the mass media concerns invasion of privacy.

72 See eg, *S v A* 1971 2 SA 293 (T); *Walker v Wezel* 1940 WLD 66; *Kidson v SA Associated Newspapers Ltd* 1957 3 SA 461 (W); *Mhlongo v Bailey* 1958 1 SA 370 (W).

73 See Neethling *Persoonlikheidsreg* 266–267; *O'Keeffe v Argus Printing and Publishing Co Ltd* 1954 3 SA 244 (C).

74 See Gross 1967 *NYULR* 34, 37–38.

privacy,[75] because there is no acquaintance with true personal facts about the person. In these instances it is the person's feelings (physical-sensory or spiritual-moral), that are involved.[76]

Physical integrity: In most instances it is justified to characterise unauthorised medical examinations and tests (such as a blood test to determine paternity or HIV status) as an infringement of privacy, since it results in an acquaintance with personal medical information about the individual. A case of this nature would also involve a violation of the body or *corpus* and thus be an infringement of physical integrity.[77]

Autonomy or self-determination: American case law considers the constitutional right to privacy to be involved when the state interferes in individuals' private lives and prescribes how they should manage their private affairs, for example if the state prescribes on issues such as religion, education of children and family planning.[78] However, it is not privacy that is involved here, but the individual's right to freely exercise his or her will, that is his or her autonomy,[79] or the capacity to live one's life as one chooses.[80]

75 As is eg done by Joubert *Grondslae* 136; Van der Merwe & Olivier 350–351; Strauss et al *Mediareg* 305; McQuoid-Mason *Privacy* 152–154.

76 Neetling *Persoonlikheidsreg* 37; De Wet & Swanepoel *Strafreg* 251 fn 128.

77 Neethling *Persoonlikheidsreg* 42.

78 See ch 2 par 3.2.1. The South African Constitutional Court also adopted this approach (see *Case v Minister of Security; Curtis v Minister of Safety and Security* 1996 3 SA 617 (CC); *National Coalition for Gay and Lesbian Equality v Minister of Justice* 1999 1 SA 6 (CC)). See further text to fn 117 below.

79 See further Neethling *Persoonlikheidsreg* 41–44, esp fn 361. For a discussion of the relationship between privacy and autonomy, see Vorstenbosch "Privacy and autonomy" 65–78. But see Burchell *Delict* 189 *et seq* 189 who argues for a wide interpretation of dignity to include the individual's right to personal autonomy.

80 See Holmes "Privacy: philosophical foundations and moral dilemma's" 18. (For his definition of privacy, see supra fn 56.) Holmes argues that it is important to distinguish between privacy and autonomy and indicates that whereas privacy is a freedom, autonomy is a power or capacity. Holmes 18–19 explains the difference between the two concepts with an example: "Suppose a person in solitary confinement for life is allowed to push a button that will randomly select one person whose life will then be monitored 24 hours a day on a television screen in his cell. Suppose that person is you. With no one to talk to, and no books, newspapers, or magazines, the prisoner's sole contact with the outside world, and his sole pastime, will be to observe you, in every detail of your life, from the most public to the most intimate. Because the prisoner has [no], and never will have, any control over you, he cannot physically constrain your choices. As measured by the absence of physical constraints, your capacity to live your life as you choose is unaffected. Your autonomy is intact, but for your inability to alter this one circumstance of your life. But you have absolutely no privacy (beyond that of your innermost thoughts, and those only as long as they

(continued...)

Patrimonial interests: Privacy must also be distinguished from patrimonial interest such as trade secrets. These two interests can easily be confused because both involve the unauthorised access to or disclosure of confidential facts. However, a trade secret is information capable of application in commerce and industry and is of real or potential value to its owner. In other words, a trade secret is a patrimonial interest, whereas privacy is a personality interest.[81]

iii Recognition of the right to privacy

Until the early twentieth century,[82] there was no reported case law in South Africa in which the right to privacy was given any substantial discussion.[83] The right to privacy was mentioned as a personality interest worthy of protection.[84] In early criminal case law, it was recognised, for example, that is an *iniuria* to enter another's house or to trespass on another's land against such person's will,[85] or to spy upon a woman through a window while she is undressing.[86] However, the courts required that the infringing action should be insulting towards the complainant and thus equated privacy with another personality interest, namely dignity.[87]

In 1954 *O'Keeffe v Argus Printing and Publishing Co Ltd*,[88] regarded as the *locus classicus* for the

80(...continued)
are never expressed)."

81 See Knobel *Trade secret* 218–219.

82 The position in Roman and Roman-Dutch law is not discussed (see Neethling *Persoonlikheidsreg* 50–61).

83 Burchell *Personality rights* 372.

84 See eg *De Fourd v Town Council of Cape Town* (1898) 15 SC 399 402; *R v Umfaan* 1908 TS 62 67.

85 *R v Schonken* 1929 AD 36.

86 *R v Schoonberg* 1926 OPD 247; *R v Holliday* 1927 CPD 395; *R v Daniels* 1938 TPD 312; *R v R* 1954 2 SA 134 (N).

87 See Neethling *Persoonlikheidsreg* 266; 1976 *THRHR* 121, 125 *et seq*. See further the discussion below.

88 1954 3 SA 244 (C).

recognition of an independent right to privacy in South African law, came before the court.[89] Ironically, in this case it was not the plaintiff's right to privacy, but her right to identity that was infringed: A photograph of an unmarried woman was published without her consent as part of an advertisement for rifles, pistols and ammunition. The court, *per* Watermeyer AJ, had to decide whether the conduct complained of was "capable of constituting a violation of plaintiff's 'real rights related to personality', and in particular, of those rights relating to her dignity".[90] The court was of the opinion that the Roman concept of *dignitas* should be given a wide interpretation[91] and be judged in the light of modern conditions and thinking.[92] After referring to English[93] and American law,[94] the court held that the unauthorised publication of a person's photograph and name for advertising purposes is capable of constituting an "aggression" upon that person's *dignitas*. According to Neethling,[95] Watermeyer AJ correctly considered the *dignitas* not as one personality interest (namely dignity which is infringed by means of an insult), but as a collective term for all the personality interests apart from the *corpus* or *fama*. This enabled the judge to include the right to privacy implicitly as one of the rights relating to *dignitas*.[96] Importantly, the court[97] also rejected the idea that *contumelia*, in the sense of "insult" is the essence of an *iniuria*,[98] thus recognising privacy as a personality interest separate from dignity.

89 Neethling *Persoonlikheidsreg* 265.

90 However, see the remarks by Harms AJA in *Jansen van Vuuren v Kruger* 1993 4 SA 842 (A) 849 with regard to the use of the term "real right" in relation to "right of personality".

91 *O'Keeffe v Argus Printing and Publishing Co Ltd* 1954 3 SA 244 (C) 247–248.

92 *O'Keeffe v Argus Printing and Publishing Co Ltd* 1954 3 SA 244 (C) 249.

93 Specifically *Tolley v JS Fry and Sons Ltd* 1930 (1) KB 467; 1931 AC 333.

94 Restatement of Torts para 867.

95 Neethling *Persoonlikheidsreg* 265.

96 This was also the conclusion of the court in *Gosschalk v Rossouw* 1966 2 SA 476 (C) 490–491.

97 Following *Foulds v Smith* 1950 1 SA 1 (A).

98 *O'Keeffe v Argus Printing and Publishing Co Ltd* 1954 3 SA 244 (C) 248.

Neethling[99] praises the decision in *O'Keeffe* for its implicit recognition of the right to privacy as an independent personality right, but is critical of the court's failure to give a comprehensive definition of the right to privacy. This resulted *in casu* in privacy being equated with another personality interest, namely identity.[100]

Other cases followed *O'Keeffe* in which the right to be free from the public disclosure of private facts[101] and the right to be free from unreasonable intrusions into the private sphere[102] were recognised.[103] Recent cases in which the former Appellate Division (now the Supreme Court of Appeal) also recognised and discussed the right to privacy include *Jansen van Vuuren v Kruger*,[104] *National Media Ltd v Jooste*,[105] *Financial Mail (Pty) Ltd v Sage Holdings Ltd*[106] and *Janit v Motor Industry Fund Administrators (Pty) Ltd*.[107]

The principles laid down in these cases can be summarised as follows:

❒ The right to privacy is recognised and protected as an independent personality right within the

99 Neethling *Persoonlikheidsreg* 265 fn 9.

100 See Neethling *Privaatheid* 376; *Persoonlikheidsreg* 265 fn 9. As will be shown, (see par 2.3.2.1 below) identity is infringed if false information is published. In order for privacy to be infringed, the facts published must be true personal information.

101 Eg *Mhlongo v Bailey* 1958 1 SA 370 (C) (unauthorised publication of a photograph of a retired schoolteacher portraying him as a young man in the company of a well-known singer); *Rhodesian Printing and Publishing Co Ltd v Duggan* 1975 1 SA 590 (R) (story about young children abducted from the custody of their parents); *La Grange v Schoeman* 1980 1 SA 885 (E) (attempted photographing of security policemen mentioned by counsel at a trial as having been responsible for the death of a detainee).

102 Eg *Gosschalk v Rossouw* 1966 2 SA 476 (C) 492 (improperly interrogating a detainee); *S v A* 1971 2 SA 293 (T) (electronically bugging a person's home).

103 See further Burchell *Personality rights* 372. For a theoretical discussion of the ways in which privacy can be infringed, see par 2.3.2.1 below.

104 1993 4 SA 842 (A).

105 1996 3 SA 262 (A).

106 1993 2 SA 451 (A).

107 1995 4 SA 293 (A).

wider concept of *dignitas*.[108]

- Neethling's definition of privacy is accepted, namely that privacy is an individual condition of life characterised by seclusion from the public and publicity; this implies an absence of acquaintance with the individual or his or her personal affairs in this state.[109]

- Both individuals and juristic persons are entitled to a right to privacy.[110]

The Bill of Rights also expressly recognises the right to privacy as a fundamental human right.[111] Section 14 of the Constitution provides:

> Everyone has the right to privacy, which includes the right not to have –
>
> (a) their person or home searched;
>
> (b) their property searched;
>
> (c) their possessions seized;
>
> (d) the privacy of their communications infringed.

This section guarantees a general right to privacy,[112] with specific protection against searches and seizures, and the privacy of communications. However, this list is not exhaustive, and it extends to any

---

108 See eg *Jansen van Vuuren v Kruger* 1993 4 SA 842 (A) 849; *O'Keeffe v Argus Printing and Publishing Ltd* 1954 3 SA 244 (C); *Universiteit van Pretoria v Tommie Meyer Films (Edms) Bpk* 1977 4 SA 376 (T) 383–384 (1979 1 SA 441 (A) 455 *et seq*); *Financial Mail (Pty) Ltd v Sage Holdings Ltd* 1993 2 SA 451 (A) 462–463 (1991 2 SA 117 (W) 129–131); *Nell v Nell* 1990 3 SA 889 (T) 895 896.

109 Neethling *Persoonlikheidsreg* 39–40; *National Media Ltd v Jooste* 1996 3 SA 262 (A) 271; *Jooste v National Media Ltd* 1994 2 SA 634 (C) 645; *Universiteit van Pretoria v Tommie Meyer Films (Edms) Bpk* 1977 4 SA 376 (T) 384; *Bernstein v Bester NO* 1996 2 SA 751 (CC) 789; *Swanepoel v Minister van Veiligheid en Sekuriteit* 1999 4 SA 549 (T) 553.

110 *Financial Mail (Pty) Ltd v Sage Holdings Ltd* 1993 2 SA 451 (A) 462–463; *Motor Industry Fund v Janit* 1994 3 SA 56 (W) 60–61; *Janit v Motor Industry Fund Administrators (Pty) Ltd* 1995 4 SA 293 (A) 304. See also *Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd* 2001 1 SA 545 (CC) 557.

111 Act 108 of 1996 s 14. On the influence of the Constitution on the law of delict in general, see par 2.2.2.

112 See also Rautenbach 2001 *TSAR* 115; Kemp 2000 *Stell LR* 437, 445.

other method of obtaining information or making unauthorised disclosures.[113]

Some commentators[114] divide the constitutional right to privacy in section 14 into "substantive privacy rights" (or "personal autonomy privacy rights")[115] and "informational privacy rights".[116] The substantive privacy rights enable individuals to make personal decisions about such interests as their family relationships, home life and sexual orientation.[117] Informational privacy rights limit the ability of people to gain, publish, disclose or use information about others without their consent.[118] Seen in this light, the constitutional right to privacy is broader than the private law right since the former also includes autonomy.

The importance of the recognition of the right to privacy as a fundamental human right is that the legislature and the executive of the state may not pass any law or take any action which infringes or unreasonably limits the right.[119] The fundamental rights may only be limited by means of a law of general application provided that the limitation is reasonable and justifiable in an open and democratic

113 McQuoid-Mason "Constitutional privacy" 18–11.

114 McQuoid-Mason 2000 *Acta Juridica* 248; Devenish *SA Bill of Rights* 147.

115 Also see ch 2 par 3.2.1.

116 Also see ch 2 par 3.2.2.

117 McQuoid-Mason 2000 *Acta Juridica* 248. Examples are: *Case v Minister of Security; Curtis v Minister of Safety and Security* 1996 3 SA 617 (CC) where it was held (per Didcott J) that a ban imposed on the possession of erotic material "invades the personal privacy which s 13 of the interim Constitution ... guarantees that I shall enjoy"; *National Coalition for Gay and Lesbian Equality v Minister of Justice* 1999 1 SA 6 (CC), where the Constitutional Court held that in so far as the offence of sodomy criminalises private conduct between consenting adults which causes no harm to anyone else, it violates the constitutional right to privacy because it intrudes on the innermost sphere of human life. The court held that "[p]rivacy recognises that we all have a right to a sphere of private intimacy and autonomy which allows us to establish and nurture human relationships without interference from the outside community". (For criticism of the equation of autonomy with privacy in this case, see Neethling 1997 *THRHR* 137, 141 *et seq*; see also par 2.3.2.1 above.) See further Rautenbach 2001 *TSAR* 115, 118 121 122.

118 McQuoid-Mason 2000 *Acta Juridica* 248. Examples of invasions of constitutional informational privacy rights include taking a prisoners's blood for DNA testing without consent (*C v Minister of Correctional Services* 1996 (4) SA 292 (T)) and restoring erased computer information (*Klein v Attorney General, WLD* 1995 3 SA 848 (W)).

119 Neethling *Persoonlikheidsreg* 21.

society.[120]

iv Infringement of privacy

Since privacy relates to personal facts which a person has determined should be excluded from the knowledge of outsiders, it follows that privacy can only be infringed when someone learns of true private facts about the person against his or her determination and will.[121]

Such knowledge can be acquired in one of two ways:[122]

- where an outsider himself or herself learns of the facts – such interference with privacy is referred to as intrusion or acquaintance[123]

- where an outsider acquaints third parties with personal facts which, although known to the outsider, nonetheless remain private – such interference with privacy is referred to as disclosure

120 Act 108 of 1996 s 36. The right to privacy can also be suspended in consequence of a declaration of a state of emergency (s 37 of the Constitution), but only to the extent necessary to restore peace and order (see Devenish *SA Bill of Rights* 137). An example of a law of general application that limits the right to privacy is the Interception and Monitoring Prohibition Act 127 of 1992. This Act prohibits the intentional interception of telecommunications or monitoring of conversations by monitoring devices unless authorised by a judge, who may authorise such actions only on specific grounds. In *S v Naidoo* [1998] 1 All SA 189 (D) 213, it was accepted that the Act is a law of general application that complies with the requirements of the limitations clause. Also see *Protea Technology Ltd v Wainer* [1997] 3 All SA 594 (W). This Act will be replaced by the Regulation of Interception of Communications and Provision of Communication-related Information Act 25 of 2002 (RICPCIA) in the near future. For a discussion of RICPCIA, see Mischke 2003 *CLL* 71. Another example of a law of general application that limits the right to privacy is the Promotion of Access to Information Act 2 of 2000 which will be discussed in ch 8.

121 Neethling *Persoonlikheidsreg* 40.

122 Neethling *Persoonlikheidsreg* 40–41; *Motor Industry Fund Administrators (Pty) Ltd v Janit* 1994 3 SA 56 (W) 60; *Bernstein v Bester NO* 1996 2 SA 751 (CC) 789. Compare *Financial Mail (Pty) Ltd v Sage Holdings Ltd* 1993 2 SA 451 (A) 462–463; also see McQuoid-Mason *Privacy* 134; Gross 1967 *NYULR* 34, 37.

123 Eg by unlawfully intruding on property, searching and seizing documents, secretly watching someone or using surveillance equipment to gather information on someone (see *S v A* 1971 2 SA 293 (T)).

or publicity[124]

Applying this distinction to the processing of personal data, it is evident that the compiling of personal information or data and obtaining knowledge thereof constitutes an act of intrusion into privacy.[125] An act of disclosure, on the other hand, is involved when the recorded information or data is subsequently distributed and thus disclosed.[126]

The "fixation" or embodiment of private facts[127] contrary to the will and determination of the plaintiff also constitutes a threat to privacy because it exposes privacy to the risk of an intrusion or exposure.[128] Collecting personal information by making a surveillance video tape would be an example of "fixation" of private information (namely where and with whom a person was at a specific time, what the person was doing, etcetera). Once the surveillance tape is made, privacy is threatened by the possibility that images from it may be viewed, disclosed or otherwise processed.

b Identity

i Definition and nature

Neethling defines identity as "a person's uniqueness or individuality which identifies or individualises him [or her] as a particular person and thus distinguishes him [or her] from others".[129] The following remarks

124 An example of an acquaintance through disclosure is eg when a doctor tells his friends about a patient's HIV status (see *Jansen van Vuuren v Kruger* 1993 4 SA 842 (A)).

125 See Dean "SA" 385.

126 Neethling *Persoonlikheidsreg* 326; "Databeskerming" 112; Du Plessis *Reg op inligting* 392.

127 This would eg include taking a picture of someone, making a tape recording of a conversation, or making a photocopy of personal documents (see Neethling *Persoonlikheidsreg* 286; Strauss et al *Mediareg* 304 306 *et seq*).

128 Neethling *Persoonlikheidsreg* 286. This view was not supported by Kotze J in *Human v East London Daily Dispatch (Pty) Ltd* 1975 2 PH J24 (E); but see *La Grange v Schoeman* 1980 1 SA 885 (E).

129 Neethling, Potgieter & Visser *Neethling's Law of personality* 39; Neethling *Persoonlikheidsreg* 44. See also (continued...)

can be made about identity as a personality interest:

- Identity is manifested in various distinguishing attributes (*indicia*) by which a particular person can be recognised.[130]

- *Indicia* are therefore facets of the personality which are characteristic of or unique to that person.[131]

- *Indicia* can on the one hand be natural attributes[132] which distinguish a person from others, such as the voice, fingerprint, appearance or physical image of a person, or on the other hand, it can be distinguishing attributes that are created by law or by the individual himself or herself, for example an identity number, a family name, a person's life history, a pseudonym, or creditworthiness.[133]

- Identity has the function of individualising a person and thus making it possible to distinguish a person from other persons.[134]

- If any of a person's *indicia* are used by another in such a manner that the true image of the person's personality is not reflected and the person can no longer be recognised for what he or she truly is, the person's identity is infringed.[135]

129(...continued)
Coetser *Identiteit* 148.

130 Neethling *Persoonlikheidsreg* 44. See also Coetser *Identiteit* 148; Joubert *Grondslae* 134.

131 Neethling *Persoonlikheidsreg* 44. Also see Coetser *Identiteit* 141.

132 In the sense that they come into existence at the birth of the person and develop naturally.

133 Coetser *Identiteit* 141; Neethling *Persoonlikheidsreg* 44.

134 Coetser *Identiteit* 145; Neethling *Persoonlikheidsreg* 44.

135 Coetser *Identiteit* 146; Neethling *Persoonlikheidsreg* 45. See also Mostert *Reklamebeeld* 292–293.

ii Identity distinguished from other interests

Identity should be distinguished from other personality interests, such as privacy, the good name, dignity and feelings, as well as from patrimonial property interests.

Privacy: Whereas privacy is infringed by an acquaintance with true personal facts about a person against the person's determination and will, identity is infringed by the untrue or false use of *indicia* of the identity.[136] Falseness is in other words the essence of identity infringement.[137] In the case of an infringement of privacy, *indicia* of the person in question can also be used, but it is merely used to identify the person with the private facts; in other words they are used in a manner that correctly reflects the person's identity.[138] If it is made known to the outside world that a person is homosexual, whereas he or she is not, the person's identity is infringed. If he or she is homosexual and that information, although known to another party is still confidential in general, is made known to a third party, his or her privacy is infringed.[139]

Privacy and identity can of course be infringed by the same conduct. For example, if an unknown person's image is used without his or her permission for advertising purposes, both privacy and identity may be involved. Privacy is infringed because a true personal fact relating to the person, namely the person's image, is disclosed against his or her will, whereas identity is infringed if a false impression is created that the person endorsed the product.[140]

---

136 Neethling *Persoonlikheidsreg* 45. The false-light tort and appropriation tort (see ch 2 par 2.1.2.3 and par 2.1.2.4) which in American law are considered to be instances of infringements of the right to privacy, are therefore actually instances of infringement of the right to identity (Neethling *Persoonlikheidsreg* 45).

137 Coetser *Identiteit* 166.

138 Neethling *Persoonlikheidsreg* 45; compare *Swanepoel v Minister van Veiligheid en Sekuriteit* 1999 4 SA 549 (T) 555.

139 See Eiselen *Reg op privaatheid in die inligtingsera* par 3.

140 Coetser *Identiteit* 168; Neethling *Persoonlikheidsreg* 46. See also Mostert *Reklamebeeld* 293.

Good name or reputation:[141] The main difference between defamation (infringement of the reputation) and identity infringement is that a statement need not be false to constitute defamation, whereas the false use of *indicia* is a prerequisite for identity infringement.[142] On the other hand, it is also evident that not every false use of the *indicium* of a person will necessarily lower the person's reputation in society – it may even have the effect of enhancing the person's reputation.[143] Furthermore, whereas publication of defamatory words or conduct is a prerequisite for defamation, publication is not a requirement for the infringement of identity.[144] For instance, where a doctor incorrectly records that a patient is HIV positive, the person's good name is not infringed as long as the doctor does not convey this information to another person. However, the person's identity is infringed.

This does not mean that identity and good name cannot be infringed by the same conduct. This will be the case, for example, where a person's photograph is published next to an article that is both false and defamatory.[145]

Dignity: Identity should also not be confused with dignity in its narrow meaning of subjective feelings of self-respect.[146] A person's dignity is infringed if the person is insulted.[147] In the case of identity infringement, insult plays no role. A person's identity can therefore be infringed if false information is recorded about him or her which portrays him or her in a favourable light.

---

141 The failure to distinguish between these two personality interests results in denying that identity exits as a separate personality interest (see Coetser *Identiteit* 169 and authority cited there).

142 Coetser *Identiteit* 169; Neethling *Persoonlikheidsreg* 46. See also Neethling 2002 *SALJ* 700, 707.

143 Coetser *Identiteit* 170 gives the example of an incorrect statement that a person has won a medal in a war.

144 Coetser *Identiteit* 170; Neethling *Persoonlikheidsreg* 46; See also Neethling 2002 *SALJ* 700, 707.

145 Coetser *Identiteit* 170.

146 Dignity is sometimes incorrectly equated with the broader concept of *dignitas* which includes all the personality rights except the rights to *corpus* and *fama*, with the result that insult or impairment of the dignity is required for every *iniuria* (see Neethling *Persoonlikheidsreg* 233). But see Burchell *Delict* 189 *et seq* and *Personality rights* 327 *et seq* who argues for a broad interpretation of dignity.

147 Neethling *Persoonlikheidsreg* 234.

Feelings: Lastly, identity should be distinguished from the individual's feelings, apart from the feelings of dignity. This personality interest includes a person's feelings in areas such as love, faith (religion), piety, sentiment and chastity. It is important to recognise that a person's identity can be infringed, irrespective of whether or not any of his or her feelings have been infringed.[148]

Patrimonial property interests: Identity is an aspect of personality and it is therefore incorrect to classify patrimonial property as falling within the ambit of this interest.[149] A distinction should therefore be made between, on the one hand, copyright, a person's advertising image and one's family name as a distinctive mark (which are all immaterial property) and identity on the other hand.[150] It stands to reason that infringement of identity can also result in the infringement of one of these patrimonial interests, but what is important is that there need not be patrimonial loss for identity to be infringed.[151]

iii Recognition of right to identity

Identity was recognised *eo nomine* for the first time in the late 1970s in *Universiteit van Pretoria v Tommie Meyer Films (Edms) Bpk*,[152] but this interest is usually protected in case law under the guise of other personality interests, such as the right to a good name and the right to privacy.[153]

148 Coetser *Identiteit* 173.

149 Coetser *Identiteit* 173; Neethling *Persoonlikheidsreg* 46–47. See also Mostert *Reklamebeeld* 293.

150 For a discussion of these distinctions, see Neethling *Persoonlikheidsreg* 25 *et seq*, 45 fn 374, 47; Coetser *Identiteit* 179–192; Van Heerden & Neethling *Unlawful competition* 110–112.

151 See further Coetser *Identiteit* 179–192.

152 1977 4 SA 376 (T): "die reg op identiteit ... word by die persoonlikheidsregte geklassifiseer" (*per* Mostert J 386).

153 See eg *O'Keeffe v Argus Printing and Publishing Co Ltd* 1954 3 SA 244 (C) and *Kidson v SA Associated Newspapers Ltd* 1957 3 SA 461 (W) (unauthorised use of a photograph for a false newspaper story). In *Swanepoel v Minister van Veiligheid en Sekuriteit* 1999 4 SA 549 (T) 553 the court held that a police informer's identity forms part of his right to privacy. This is correct of course, since his identity is not falsified, but merely used to match the person with certain information that he has knowledge of. Also see Neethling 2000 *TSAR* 761–765.

As was stated previously,[154] identity is not recognised *eo nomine* in the Bill of Rights, but it can be considered to be protected under the right to dignity which is mentioned explicitly in section 10. This has happened in the case of the right to a good name (*fama*) which is also not mentioned explicitly, but is regarded as part of the right to dignity.[155] The concept of human dignity in the Constitution can thus be compared with the broad *dignitas* concept of common law.[156]

It has been pointed out that the importance of the recognition of a personality right as a fundamental human right is that the legislature and executive of state may not pass any law or take any action which infringes or unreasonably limits the right, since the fundamental rights may only be limited by means of a law of general application that is reasonable and justifiable in an open and democratic society.[157]

iv Infringement of identity

A person's identity is infringed if any of his or her *indicia* are used without authorisation in a way which cannot be reconciled with his or her true image.[158] In other words, identity is infringed by a misrepresentation or falsification of the true identity of an individual.

---

154 See par 2.2.2.

155 See *Van Zyl v Jonathan Ball Publications (Pty) Ltd* 1999 4 SA 571 (W) 591; *Marais v Groenewald* 2001 1 SA 634 (T) 646; *Van den Berg v Coopers & Lybrand Trust (Pty) Ltd* 2001 2 SA 242 (SCA) 253; *National Media Ltd v Boghoshi* 1998 4 SA 1196 (SCA) 1216–1217; *Bogoshi v National Media Ltd* 1996 3 SA 78 (W) 82; *Holomisa v Argus Newspapers Ltd* 1996 2 SA 588 (W) 606; *Gardener v Whitaker* 1995 2 SA 672 (E) 690–691; also see Burchell *Personality rights* 139; Neethling, Potgieter & Visser *Delict* 337 fn 104; Neethling *Persoonlikheidsreg* 95–96; Neethling & Potgieter 1994 *THRHR* 513, 516. This is likely to happen, especially since identity is part of the broad *dignitas* concept in private law and human dignity is recognised as a fundamental democratic value in the Constitution. Furthermore, the Bill of Rights does not negate the existence of other rights and freedoms already recognised at common law or by statute as long as these rights are not in conflict with the Bill of Rights. Also see See McQuoid-Mason 2000 *Acta Juridica* 227, 231.

156 See par 2.1. But see fn 32.

157 See par a.iii above.

158 Coetser *Identiteit* 163; Neethling *Persoonlikheidsreg* 45.

The following two "torts" in American law[159] can serve as examples of infringement of identity as an *iniuria*:[160]

- the public falsification of the personality image (described as "publicity which places the plaintiff in a false light in the public eye", or the "false-light tort")

- the economic misappropriation of identity *indicia*, especially for advertising purposes (described as "appropriation, for the defendant's advantage, of the plaintiff's name or likeness", or the "appropriation tort")[161]

An example of the false-light situation of identity infringement is where a data controller (credit bureau) gives out false information about the creditworthiness of a data subject to a third party. In this regard it must be emphasised that the American legal position that only a public disclosure is wrongful is too absolute. The disclosure of false information to only one person could also be wrongful.[162]

The appropriation tort only infringes identity to the extent that the economic misappropriation of the *indicia* creates the false impression that the person in question has consented to the conduct, or has received financial remuneration therefor or supports the advertised product, service or business.[163] An example of this type of identity infringement is where a person's name and address is used on a mailing list without his or her consent.

Another example of appropriation of identity that is one of growing concern, is "identity theft" – a

159 See ch 2 par 3.2.1.

160 In American law these torts are considered to be protecting the right to privacy. Our courts have followed the American approach in *O'Keeffe v Argus Printing and Publishing Co Ltd* 1954 3 SA 244 (C) and *Kidson v SA Associated Newspapers Ltd* 1957 3 SA 461 (W) where the right to identity was protected under the guise of the right to privacy (see above).

161 Neethling *Persoonlikheidsreg* 45–46; Neethling, Potgieter & Visser *Delict* 357.

162 See par 2.3.2.2 below. See also Neethling *Persoonlikheidsreg* 310.

163 Coetser *Identiteit* 181; Mostert *Reklamebeeld* 181; Neethling *Persoonlikheidsreg* 45–46.

person appropriates another's person's identity for himself or herself in order to fraudulently obtain a financial benefit, such as credit.[164]

It must, however, be emphasised that publication is not a requirement for infringement of identity. The mere falsification of data is sufficient.

Identity can only be infringed if the personality image has been falsified. This means that if the representation made is in fact true, the conduct does not amount to an infringement of identity.[165] The literal truth is not the real issue, however, but whether the impression created is correct. For example, where a credit reference agency states that a specific person has not paid his or her debts for three months, but neglect to mention that the person was unconscious during that period as a result of a car accident, the statement is factually true, but portrays a false image of the person as posing a bad credit risk.[166] In other words, the information should not create a misleading image and should fully reflect the person's situation.

It should also be kept in mind that where the image created is so false that the person cannot be recognised from it, the person's identity is not infringed. Infringement of identity occurs only if the false identity can be connected to someone.[167] Furthermore, the misuse of only one of the *indicia* of a person might not be sufficient to create a recognisable connection with the particular person.[168]

164 See eg Solove "Identity theft" 303, 321. An example would be where a "hacker" obtains the password of a person to the person's bank account, and then uses that password to access the account and withdraw money from the account.

165 See Neethling *Persoonlikheidsreg* 309; Coetser *Identiteit* 195.

166 Coetser *Identiteit* 195–196; Neethling *Persoonlikheidsreg* 308.

167 Coetser *Identiteit* 197; Neethling *Persoonlikheidsreg* 309.

168 Coetser *Identiteit* 197; Neethling *Persoonlikheidsreg* 309. Neethling therefore argues that the use of corresponding names cannot by itself be an infringement of identity. Where a writer gives the name of a real-life person to a fictitious character in a book, infringement of identity will only be present if there are sufficient indications that a reasonable average reader would notice the resemblance between the fictitious character and the real person.

Data processing would therefore infringe the individual's identity when inaccurate data (that is, data that are incorrect or misleading as to any matter of fact[169]) on a person are processed, because in such circumstances personal information is used in a manner that is not in accordance with the person's true image.[170] For instance, if it is incorrectly recorded or reported that a person is HIV-positive, the person's identity is infringed. This illustrates that both the recording and the disclosure of incorrect data constitute independent ways of infringing identity.

2.3.2.2 Violation of a norm

Not every factual infringement of the personality will be wrongful, however. As stated previously, in order for an infringement of the personality to be wrongful, there must, apart from a factual infringement of the personality, also be a violation of a norm (that is, the prejudice must have occurred in a legally reprehensible or unreasonable manner).[171]

a Criterion of wrongfulness

Whether a factual infringement of a personality interest (in our case, either privacy or identity) should be considered to be wrongful, is determined by means of the *boni mores* or legal convictions of the community.[172] It is an objective test based on the criterion of reasonableness.[173]

Since it is an objective test, subjective factors such as the defendant's honesty, *bona fides*, motive or knowledge are generally not relevant in determining wrongfulness. But in certain exceptional cases these

169 See eg DPR *Data Protection Act 1998* 14.

170 See also Neethling *Persoonlikheidsreg* 326.

171 Neethling, Potgieter & Visser *Delict* 35; Van der Merwe & Olivier *Onregmatige daad* 29.

172 Neethling, Potgieter & Visser *Delict* 37–38; McQuoid-Mason "Constitutional privacy" 18–2; Van der Walt 1993 *THRHR* 558, 563.

173 Boberg *Delict* 30 *et seq*; Burchell *Delict* 24 *et seq*; Neethling, Potgieter & Visser *Delict* 38; Van der Walt & Midgley *Delict* 55 (par 56).

subjective factors may become relevant.[174]

The application of the *boni mores* criterion essentially entails the *ex post facto* balancing or weighing up of the opposing interests involved. In other words, the interests of the defendant must be weighed against those of the plaintiff in the light of all the relevant circumstances and in view of all pertinent factors.[175] It must then be decided whether the infringement of the plaintiff's interests to promote the interests of the defendant, if any, was reasonable.[176]

According to Joubert, the *boni mores* criterion as a yardstick for determining wrongfulness is of particular value in the area of *iniuria*, since this criterion makes it possible to adapt *inuiria* to changing views by the community on what is right and proper as the level of cultural development rises. Furthermore, the criterion helps to define the limits of the protection afforded to the personality.[177]

However, as Knobel indicates, the very same qualities that make the *boni mores* such an extraordinary useful general criterion for delictual wrongfulness may limit its usefulness in specific instances, because its vagueness makes it difficult to apply with predictability and consistency to specific factual

174 See Neethling, Potgieter & Visser *Delict* 44–45. According to the doctrine of abuse of rights, an improper motive may be indicative of unreasonable and thus unjustifiable conduct. Eg, in defamation cases malice on the part of the defendant destroys the defence of privilege (Van der Walt & Midgley *Delict* 56 (par 56)). See also Neethling, Potgieter & Visser *Delict* 40 44–46.

175 Including legal policy considerations (see Van Aswegen 1993 *THRHR* 171, 179 180; Corbett 1987 *SALJ* 52 *et seq*). The following policy considerations have been identified as factors that play a role in determining the reasonableness of the defendant's conduct: the nature and extent of the harm and of the foreseeable or foreseen loss; the possible value to the defendant or to society of the harmful conduct; the costs and effort of steps which would have to be taken to prevent the loss; the degree of probability of the success of the preventive measures; the nature of the relationship between the parties; the motive of the defendant; economic considerations, the legal position in other countries; ethical and moral issues; the values underlying the Bill of Rights; as well as other considerations of public interest or public policy. See also *Administrateur, Transvaal v Van der Merwe* 1994 4 SA 347 (A) 361–362. On the influence of the Constitution on the *boni mores*, see par 2.2.2. See also Neethling *Persoonlikheidsreg* 68–69; Neethling, Potgieter & Visser *Delict* 40 fn 22.

176 Neethling, Potgieter & Visser *Delict* 39; Boberg *Delict* 33; Snyman *Criminal law* 91; Van der Walt & Midgley *Delict* 55 (par 56); Van der Walt 1993 *THRHR* 558, 563–564.

177 Joubert *Grondslae* 109. See also Neethling *Persoonlikheidsreg* 68; McQuoid-Mason *Privacy* 116 *et seq;* Neethling, Potgieter & Visser *Delict* 41.

situations.[178] Over the years, more precise methods have therefore been developed to ascertain the legal convictions of the society, so that the general *boni mores* criterion need not be applied directly to establish wrongfulness in each individual case.[179] Of great practical importance in this regard are the grounds of justification.[180]

The practical application of the *boni mores* criterion is furthermore facilitated by two tests to determine wrongfulness. First of all, in some instances wrongfulness is determined by reference to the subjective rights doctrine.[181] In terms of this doctrine an infringement of a subjective right is wrongful. This means that in general, the fact that an infringement of a legally recognised interest has occurred is already an indication of the wrongfulness of the conduct.[182] The doctrine of subjective rights is of particular importance for data processing since the personality rights to privacy and identity are subjective rights, the infringement of which is wrongful.

In South African law wrongfulness is also determined with reference to the breach of a legal duty.[183] In such instances the question asked is not whether the plaintiff's rights have been infringed, but rather whether the defendant had a legal duty to prevent the loss.[184] However, "breach of a duty and infringement of a right are not alternative foundations for a finding of wrongfulness. Rather they are

178 Knobel *Trade secret* 238–239. Also see Boberg *Delict* 33; Snyman *Criminal law* 91.

179 The general *boni mores* criterion is only directly applied in exceptional circumstances. Eg, in novel situations where there is no clear legal norm or ground of justification involved and also for refinement in borderline situations where wrongfulness is difficult to determine (Neethling, Potgieter & Visser *Delict* 46).

180 See par 2.3.2.3

181 This doctrine was accepted by the court in *Universiteit van Pretoria v Tommie Meyer Films (Edms) Bpk* 1977 4 SA 376 (T) 387.

182 Neethling, Potgieter & Visser *Delict* 54; Van der Merwe & Olivier *Onregmatige daad* 50. See also Snyman *Criminal law* 91.

183 Boberg *Delict* 31; Neethling, Potgieter & Visser *Delict* 55–56; Van der Walt & Midgley *Delict* 55 (par 56); Van der Walt 1993 *THRHR* 558, 559.

184 This test is specifically used in cases of determining liability for an *omission*, or for the causing of pure economic loss (see further Neethling, Potgieter & Visser *Delict* 56 *et seq*; Scott 2001 *THRHR* 681, 685; Van der Walt & Midgley *Delict* 70 (par 60)).

alternative paths to the policy conclusion that the wrongfulness requirement compels, the one or the other seeming more comfortable in the circumstances".[185]

Where there is a legal duty on the processor not to process personal data, such processing is naturally wrongful. Processing data in breach of a statutory provision or in breach of the duty of a public authority to act within its powers (*ultra vires* rule) or in breach of a contractual agreement is also indicative of wrongfulness.[186]

The criterion of reasonableness (or what society recognises as reasonable) is also the yardstick the Constitutional Court utilises to determine the wrongfulness of an infringement of privacy. In this regard the scope of the constitutionally protected right to privacy is determined by the interpretation given to this right in the Constitution.[187] The constitutional (informational) right to privacy has been interpreted by the Constitutional Court as coming into play wherever a person has the ability to decide what he or she wishes to disclose to the public.[188] In other words, it extends to those aspects of a person's life in regard to which he or she has a legitimate expectation of privacy.[189] In *Protea Technology v Wainer*[190] Heher J said that whether a legitimate expectation of privacy exists, depends on whether the person has

185 Boberg *Delict* 32. Eg, Meiring *Betalingstelsel* 344 indicates that "[b]y die skending van die bankgeheim word die klem eerder op die verbreking van die swygplig van die bank gelê, as op die kliënt se reg op privaatheid".

186 See ch 4 par 4.3.4.2 and ch 5 par 4.3.4.

187 The interpretation given to privacy in a private law context is of course also instructive in interpreting the constitutional privacy right (see *Bernstein v Bester NO* 1996 2 SA 751 (CC)). Neethling *Persoonlikheidsreg* 97 points out that just as the interpretation and application of the fundamental rights will have an influence on the delictual protection of personality rights, the converse will also take place. The Bill of Rights contains many concepts which are already well-known in private law and it is only natural that courts will have regard to the meaning they have acquired in private law and apply that in the development of constitutional protection. Also see McQuoid-Mason "Constitutional privacy" 18–2.

188 See *Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd* 2001 1 SA 545 (CC) 557. The court added that the expectation that such a decision will be respected must be reasonable.

189 *Bernstein v Bester NO* 1996 2 SA 751 (CC) 792; *Protea Technology Ltd v Wainer* [1997] 3 All SA 594 (W) 608; 1997 9 BCLR 1225 (W) 1241. See also Currie & Klaaren *AIA commentary* 116–117 (par 8.2).

190 *Protea Technology Ltd v Wainer* [1997] 3 All SA 594 (W); 1997 9 BCLR 1225 (W) 1241. Also see *Waste Products Utilisation (Pty) Ltd v Wilkes* 2003 2 SA 515 (W) 551.

a subjective expectation of privacy which society recognises as reasonable. This links up with the private law view of the protection of privacy, namely that the person subjectively determines the extent of his or her right to privacy, and that the *boni mores* recognise this determination as reasonable.

In *Bernstein v Bester*[191] the court held that an expectation of privacy in relation to an individual's body, home and family-life and intimate relationships is reasonable,[192] but that as a person moves into communal relations and activities such as business and social interaction, the scope of personal space shrinks accordingly.[193] The court also held that "[t]he nature of privacy implicated by 'the right to privacy' relates only to the most personal aspects of a person's existence, and not to every aspect within his/her personal knowledge and experience", and "[i]n the context of privacy ... it is only the inner sanctum of a person such as his/her family life, sexual preference and home environment which is shielded from erosion...".[194] But in *Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd*[195] Langa DP interpreted *Bernstein* not to say that moving beyond the established "intimate core" negates the existence of a right to privacy in the social capacities in which people act. The court held that even when people are in their offices, in their cars or on mobile telephones, they still retain a right to privacy.[196]

191 *Bernstein v Bester NO* 1996 2 SA 751 (CC).

192 *Bernstein v Bester NO* 1996 2 SA 751 (CC) 788.

193 *Bernstein v Bester NO* 1996 2 SA 751 (CC) 788.

194 *Bernstein v Bester NO* 1996 2 SA 751 (CC) 788 789. Neethling 1997 *THRHR* 137, 140 argues that this definition of privacy is too narrow. He warns that care should be taken in defining the constitutional right to privacy. Too narrow an interpretation may lead to a negation of aspects of privacy that are in need of protection, such as the collection of personal information where all or some of the data are not always of a very personal nature and cannot always even be considered as private according to his definition of privacy, but the total picture created by the record of the information is of such a nature that the person would like to restrict access to it on the part of others.

195 2001 (1) SA 545 (CC) 557.

196 In *Protea Technology Ltd v Wainer* [1997] 3 All SA 594 (W) 609 [1997 9 BCLR 1225 (W)] the court (per Heher J) held that an employee has a legitimate expectation of privacy when making private phone calls at the office. "Although he must account to his employer if so required for the time so spent, the employer cannot compel him to disclose the substance of such calls ... However, telephone calls of the employee relating to the employer's affairs are not private and are not protected under the Constitution." Also see Johnson 2000 (Nov) *De Rebus* 54 and Mischke 2003 *CLL* 71 for a discussion of the implications of

(continued...)

Since the Constitutional Court recognises that the right to privacy in section 14 of the Constitution includes "informational privacy", it is submitted that a person has a reasonable expectation of privacy in respect of private information and that limits should therefore be imposed on the collection and use of individual pieces of personal information that on their own are not private but if collected create a private profile of a person.[197] Seen in this light it is submitted that the constitutional protection of the right to privacy places a duty on the state to adopt proper measures for the protection of personal data.[198]

Next it will be established how the *boni mores* ought to evaluate, in specific circumstances, the processing of personal data that factually infringe the privacy or the identity of the individual.

b Wrongfulness of infringement of privacy

As has been said,[199] privacy is infringed by either an act of intrusion or an act of disclosure, since privacy is infringed where outsiders are acquainted with true personal facts about a person, contrary to the determination and will of that person. Where such an infringement is also *contra bonos mores*, the infringement will be wrongful.

As will be demonstrated, the distinction between acts of intrusion and acts of disclosure is also of importance in the area of data processing in determining the wrongfulness or not of such processing.

196(...continued)
workplace monitoring of e-mail and phone calls.

197 The expectation of privacy must be reasonable in the circumstances of the case – a person may not, for example, refuse to provide identification to a police official when so requested (De Waal, Currie & Erasmus *Bill of Rights* 250 referring to *S v Zwayi* 1998 (2) BCLR 242 (Ck)). Similarly, when an individual is under police investigation the police may lawfully compile a dossier or file on the individual. The scope of the right to privacy also has to be demarcated with reference to the rights of others and the interests of the community (*Bernstein v Bester NO* 1996 2 SA 751 (CC); *Mistry v Interim Medical and Dental Council of South Africa* 1998 (4) SA 1127 (CC)).

198 Neethling *Persoonlikheidsreg* 327; 2002 *THRHR* 574, 589.

199 Par 2.3.2.1.a.iii.

i Intrusion

In the case of an act of intrusion, Neethling[200] distinguishes between acquaintance with private facts that are totally excluded or limited to specific persons on the one hand and private facts limited to an indeterminate but limited number of persons on the other hand. Public records are of course not private, but the use of information from such records to compile profiles on people might present problems from a data protection point of view and is therefore also considered here.

❒ Acquaintance with private facts totally excluded or limited to specific persons

Here one is dealing with information that is characterised by an element of confidentiality, for example information contained in private documents, in a private conversation, or in a private electronic-mail message, or information obtained as a result of a medical examination or blood test.[201] Neethling suggests that almost every unauthorised acquaintance with private facts in these instances may in the absence of justification be regarded as wrongful.[202] In other words, collecting personal information by accessing private or confidential documents,[203] by eavesdropping on private conversations, by intercepting private e-mail messages or by running unauthorised medical tests will in principle be wrongful. In every instance, however, one has to consider the surrounding circumstances. In a specific instance the dictates of society may result in conduct, such as eavesdropping on a private conversation, not being wrongful, for example because the person was in a situation where he or she could not help overhearing the private conversation. If the intrusion is of a trivial nature, the maxim *de minimus non curat lex*[204] should be taken into consideration.

---

200 Neethling *Persoonlikheidsreg* 269 *et seq*.

201 Other examples of this type of privacy infringement include intrusion into a private residence and secretly watching persons.

202 Neethling *Persoonlikheidsreg* 270.

203 Eg, by reading a person's personal letters, or his or her financial statements at a bank, or a doctor's medical file on the patient.

204 The law does not concern itself with trifles (*Dig* 4.1.4).

❒ Acquaintance with private facts available to an indeterminate but limited number of persons

Where private facts are available to an indeterminate, but limited, number of persons, the position regarding the wrongfulness of an intrusion into such information is different. Since the person determines the information to be available to outsiders, acquaintance with it should in principle not be wrongful, unless the circumstances are such that the *boni mores* dictate the conduct to be wrongful.[205]

As far as data processing is concerned, however, it is submitted that the unauthorised collection or storage of personal information, and therefore acquaintance with such information, is in principle *contra bonos mores* and thus *prima facie* wrongful.[206] As Neethling convincingly points out, no person has to tolerate information concerning him or her being collected.

It is submitted, however, that an exception should be made in the case of the collection of information for merely personal, domestic use. The compiling of a mailing list on your friends and family in order to send out birthday or Christmas cards should not be *prima facie* wrongful, even if such list is kept in a database on a personal organiser.[207]

❒ Acquaintance with private facts in records that are open to the public

Personal information contained in documents that are open to the public (such as court records or records available on the Internet) may of course be accessed by outsiders, since the information has lawfully been made public. However, where a person, after an extensive computerised search of these publicly accessible records, compiles a dossier or file on another person, such conduct should be

---

205 See Neethling *Persoonlikheidsreg* 273. Neethling gives the example of observing a person in a public place. In principle, this is not wrongful, since the person has, by going out into public, determined that such acquaintance can take place. However, where such observation is part of the constant shadowing of the person, the *boni mores* would consider the conduct to be wrongful.

206 Also see Neethling *Persoonlikheidsreg* 326.

207 The *boni mores* are determinative of wrongfulness in "grey areas" such as this – if the view of the majority of society changes one might reach a point where even such collections could become unacceptable unless the persons on the list has consented to their inclusion.

considered to be *prima facie* wrongful, since the nature of the information changes. What used to be isolated pieces of unrelated information now becomes an extensive profile of a person, not envisaged when the initial documents were made available.[208] Such conduct can be compared to the constant "shadowing" of a person. It is acceptable to briefly watch a person who appears in public, but when one starts to constantly follow such a person and is able to account for all his or her movements, the "shadowing" becomes unreasonable and thus wrongful.[209]

ii Disclosure

As far as an act of disclosure is concerned, a distinction is made between three types of disclosure, namely disclosure of private facts acquired by a wrongful act of intrusion; disclosure of private facts meant only for specific people; and disclosure of private facts through mass publication.[210] Lastly, the wrongfulness of a fixation of personal information is also examined.

❒ Disclosure of private facts acquired by wrongful act of intrusion

Where a person has acquired private facts by a wrongful act of intrusion, it stands to reason that any subsequent disclosure will also be wrongful. In other words, accepting that the collection of personal information is wrongful, any subsequent processing (such as using or disseminating) will also in principle

208 See eg *Department of Justice v Reporters Committee for Freedom of the Press* 489 US 749 (1989) 763–764 where the US Supreme Court found that an individual's privacy can be infringed by the disclosure of that person's "rap sheet" (criminal record), although all the information (arrests, indictments, convictions, and sentences) summarised in a "rap sheet" has been previously disclosed to the public. The court held that "the compilation of otherwise hard-to-obtain information alters the privacy interests implicated by disclosure of that information. Plainly there is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information". The court also emphasised the role of the computer in compiling information: "The privacy interest in a rap sheet is substantial. The substantial character of that interest is affected by the fact that in today's society the computer can accumulate and store information that would otherwise have surely been forgotten long before a person attains the age of 80, when the FBI rap sheets are discarded." Also see ch 2 par 3.2.2. See further Currie & Klaaren *AIA commentary* 128 (par 8.20).

209 Neethling *Persoonlikheidsreg* 273 329; 1980 *THRHR* 141, 148.

210 Neethling *Persoonlikheidsreg* 274.

(in the absence of a ground of justification) be wrongful.[211]

❒ Disclosure of private facts meant only for specific people

It is more problematic to determine wrongfulness where personal information was made available to one or more outsiders, but the person making the personal information available had still determined that the information should remain private and should not be disseminated any further. According to Neethling, if the information is further disclosed to only one person or a small group of persons, such disclosure is as a rule not wrongful, since it is part of life that people gossip about one another and as such the disclosure cannot be considered to be wrongful.[212]

However, where a person imparts personal information to another while in a confidential relationship with the other person, a disclosure contrary to the confidential relationship would be wrongful.[213] For example, if a patient discloses personal information to his or her doctor (either by informing the doctor verbally of personal details, or by allowing the doctor to examine him or her and thus disclosing personal physical information), the doctor may not without authorisation disclose such information to another person, such as the patient's spouse or partner.[214] Other relationships that have been recognised as confidential relationships, are the relationship between husband and wife, legal adviser and client,[215] banker and client,[216] priest and penitent, and public servant and citizen.[217] These

211 This accords with the *boni mores* and has been accepted by South African courts (see eg *Financial Mail v Sage Holdings Ltd* 1993 2 SA 451 (A) 463). See further Neethling *Peroonlikheidsreg* 274, 326.

212 Neethling *Persoonlikheidsreg* 275.

213 Neethling *Persoonlikheidsreg* 276.

214 An example is where a doctor establishes that a patient is HIV positive. The doctor may only reveal such information if there is a valid ground justifying his or her actions.

215 The confidential relationship between attorney and client is the only relationship protected by an absolute legal testimonial privilege (Van Dokkum 1996 *De Rebus* 748).

216 See Meiring *Betalingstelsel* 342–372. On the banker's duty of secrecy in German, English, American and South African law, see Faul *Bankgeheim*.

217 Neethling *Privaatheid* 61 *et seq* 70 *et seq* (Germany); 138 *et seq* 142 (France); 203 *et seq* (USA); 252 *et seq*
(continued...)

relationships should not be regarded as a *numerus clausus*. Rather, one should identify the principle that all these relationships have in common and on that basis extend this rule to other relationships. The common basis in all these instances is that the relationship is such that one of the parties is compelled to disclose personal information about himself or herself to the other party. Neethling therefore suggests that a useful yardstick to determine the *boni mores* in these instances is to establish the extent to which it is necessary for one person to impart private facts to an outsider. The more necessary it is, the more pressing the protection against the disclosure of those facts to third parties by the outsider should be.[218] In such a relationship a legal duty of confidentiality rests on the person to whom the information is disclosed. It should be recognised that this duty not to disclose is the reverse of the other party's right to privacy.[219]

A confidential relationship worthy of protection may also arise as a result of of a valid contractual agreement between parties that private facts will not be disclosed. Breach of such an agreement will, apart from a breach of contract, also result in an infringement of the right to privacy.[220]

The above principles also apply to data processing. For example, where personal information is imparted to a doctor, banker or the state, the latter may not disclose the information for any other purpose than the purpose it was originally furnished for.[221]

Neethling[222] suggests that where a person lawfully[223] takes a photograph or makes a tape or video

217(...continued)
(England); Neethling *Persoonlikheidsreg* 276.

218 Neethling *Persoonlikheidsreg* 276. Neethling follows Giesker (Giesker H *Das Recht der Privaten an der eigenen Geheimsphäre* (1905)) in this regard.

219 Neethling *Persoonlikheidsreg* 276–277; Meiring *Betalingstelsel* 344; Faul *Bankgeheim* 460 *et seq*.

220 Neethling *Persoonlikheidsreg* 277. Also see ch 4 par 4.3.4.2.

221 Such a view complies with the purpose specification principle (see ch 6 par 2.2.2).

222 Neethling *Persoonlikheidsreg* 277 fn 82. On fixation, see below.

223 Eg because the person has granted permission, or because making the recording is necessary to protect
(continued...)

recording of someone,[224] unauthorised publication (disclosure) of such photograph or recording should be considered wrongful, even where the disclosure is to a small number of persons. In regard to data processing, this would mean that where a data controller lawfully operates a video surveillance camera, such surveillance footage may not be disclosed unless a legitimate ground of justification is present, such as the consent of the data subject or statutory authority in the form of a warrant.

❒ Disclosure of private facts through mass publication

Neethling suggests that the mass publication of personal information is in principle *contra bonos mores* and thus, in the absence of justification, wrongful.[225] He argues that no person needs to tolerate the mass publication even of his or her image, for example, if this is contrary to his or her determination.[226] The type of publications envisaged under this heading (namely publication by the mass media) does not concern data processing issues and consequently need not be discussed further.

In all of the above circumstances the act of intrusion or disclosure should of course be judged in context, taking into account all the surrounding circumstances.[227]

❒ Fixation or embodiment of private facts

Neethling[228] also considers the fixation, or embodiment, of private facts (for example taking a picture of someone, making a tape recording of a conversation, or making a photocopy of personal documents)

223(...continued)
other legitimate interests.

224 This is referred to as fixation or embodiment of private facts (see below).

225 Neethling *Persoonlikheidsreg* 280. But see *Financial Mail v Sage Holdings Ltd* 1993 2 SA 451 (A) where the court refrained from expressing an opinion in this regard.

226 Support for this view is to be found in positive law (see *inter alia O'Keeffe v Argus Printing and Publishing Co Ltd* 1954 3 SA 244 (C)).

227 Neethling *Persoonlikheidsreg* 286.

228 Neethling *Persoonlikheidsreg* 286.

contrary to the will and determination of the plaintiff, to be wrongful, because it constitutes a threat to the right to privacy. Even where a person is authorised to be acquainted with private facts, the unauthorised fixation of such facts should in principle be considered wrongful, because it is contrary to human nature.[229]

An example would be if a security company is contracted by a business to install a video surveillance camera in order to monitor access to their building. Should the security company then decide to make tape recordings of the people entering and leaving the building and to digitally store the recording on a computer, they are *prima facie* unlawfully making an embodiment of private information.

Summary

In conclusion, the following conduct with regard to processing of personal data should be considered to be *prima facie* wrongful, because it infringes on a person's privacy in a *prima facie* unreasonable manner:

- collecting personal information through unlawful means (unlawful intrusion into privacy), for example by accessing private or confidential documents, by eavesdropping on private conversations, intercepting private electronic-mail messages or running unauthorised medical tests, as well as any subsequent disclosure of such data

- compiling a dossier or file on another person, including private as well as public personal facts (excluding compiling for mere personal use), as well as subsequent disclosure thereof

- disclosing information collected from an individual in breach of a confidential relationship

229 Neethling *Persoonlikheidsreg* 287. Note, however, that the secret taping of a conversation by one of the parties to a conversation does not infringe the other party's right to privacy. Disclosure of the taped conversation, on the other hand, would be *prima facie* wrongful. For a discussion of this issue, see Neethling 2001 *THRHR* 131, 133.

- fixation of personal information, as well as any subsequent disclosure of such facts

- disclosing personal data which have been obtained through authorised fixation thereof

c Wrongfulness of infringement of identity

Identity is infringed by conduct that misrepresents the personality of the person. For the purpose of determining wrongfulness, Coetser[230] distinguishes between three types of misrepresentation, namely the act of falsification itself (including fixation of false information), the publication of the misrepresentation to individuals or a small group of people and publicity or publication of the misrepresentation to an unlimited number of people (mass publication).

i Falsification of facts

Here one is concerned with the act of falsifying the image, even before this has come to the notice of third parties, for example by changing correct information recorded on someone, or by recording incorrect information on someone. This conduct should *prima facie* be regarded as wrongful, since it constitutes a serious infringement of a person's identity.[231] Recorded false facts that are subsequently used result in a continuous infringement of the personality of the person involved.[232]

The maxim *de minimus non curat lex* should of course be taken into consideration and a trivial fault in the recorded information or the deletion of irrelevant personal information should not be actionable.[233]

230 Coetser *Identiteit* 197.

231 Such a view is in conformity with the data quality principle (see ch 6 par 2.2.3).

232 See Coetser *Identiteit* 198; Neethling *Persoonlikheidsreg* 310.

233 See Coetser *Identiteit* 199; McQuoid-Mason *Privacy* 207; Neethling *Persoonlikheidsreg* 310.

ii Disclosure of false information to individuals or a small group of people

Where incorrect information about someone is conveyed to a small number of persons, Neethling argues that such conduct is not *per se* wrongful, because it is a fact of life that people gossip and in the process convey incorrect information.[234] Coetser opines that the situation is different, however, where there is a duty on someone to give out the correct information. In such an instance the *boni mores* would consider it to be wrongful if the person on whom the duty to tell the truth[235] rests should give out false or misleading information. A duty to tell the truth rests on a person in those situations where he or she has specific knowledge about another person (the data subject) owing to the fact that they are in a special relationship,[236] or owing to the fact that the first person occupies a specific office or position giving him or her this special knowledge.[237]

The issuing of false and misleading information by, for example, a credit reference company on a data subject, a bank on a client, an employer on an employee, and a doctor on a patient should therefore be considered to be wrongful.[238]

iii Mass publication of false information

The mass publication of false facts about a person is in principle *contra bonos mores* and therefore *prima facie* wrongful. No person has to tolerate false information regarding himself or herself being disseminated to the public.[239] However, this type of publication does not typically involve data

234 Neethling *Persoonlikheidsreg* 310. See also Coetser *Identiteit* 198. The importance of freedom of speech in society should also be recognised in this regard.

235 Coetser *Identiteit* 201–202 refers to this as a *waarheidsplig*.

236 Eg, a banker-client, or employer-employee relationship.

237 Eg, if an official of the bar association is asked for a certificate on the standing of an advocate as a member of that bar, the person issuing such certificates has a duty to supply correct information.

238 Coetser *Identiteit* 201–202; Neethling *Persoonlikheidsreg* 310–311.

239 Neethling *Persoonlikheidsreg* 311. See also Coetser *Identiteit* 203.

processing, and consequently need not be discussed further.[240]

Summary

In conclusion, it can be said that the recording, use and publication of false personal data by a data controller should in principle be wrongful, because it infringes the right to identity. Data controllers should therefore be under a duty, as the reverse side of the right to identity, not to process false data. A breach of this duty is *contra bonos mores* and therefore wrongful.

2.3.2.3 Grounds of justification

a Introduction

It is important to remember that the *prima facie* wrongfulness of an intrusion into privacy or the infringement of identity may be excluded by the presence of a ground of justification.[241] In other words, the data processing involved may take place lawfully, provided that there is a ground that justifies the processing.[242] In reality, grounds of justification are the practical expression of the *boni mores* or reasonableness criterion with reference to typical factual circumstances which occur regularly in practice[243] – they "are situations in which the legal convictions of the community have, over the years, crystallized in the form of judicial pronouncements".[244] Because grounds of justification are

240 Similar to the infringement of privacy through mass publication of private facts (see above).

241 A distinction should be made between defences directed at the wrongfulness element and those that serve to exclude fault. A ground of justification excludes the wrongfulness of a defendants's conduct (see Van der Walt & Midgley *Delict* 95 (par 78); *May v Udwin* 1981 1 SA 1 (A) 10; *Ramsay v Minister van Polisie* 1981 4 SA 802 (A) 807; *Bernstein v Bester NO* 1996 2 SA 751 (CC) 790).

242 Also see the data protection principle of fair and lawful processing (ch 6 par 2.2.1).

243 Neethling, Potgieter & Visser *Delict* 75–76; Van der Walt & Midgley *Delict* 95 (par 78).

244 Burchell *Delict* 67.

embodiments of the *boni mores*, the existing grounds do not form a *numerus clausus*.[245]

The traditional grounds of justification recognised in South African law are consent, private defence, necessity, impossibility, provocation, statutory or official capacity, and power to discipline.[246] For defamation, which also involves an infringement of the personality, the following additional grounds of justification are recognised: privilege, truth and public benefit, fair comment and reasonable publication.[247] In instances of mass publication of private facts, the public interest in information may also serve as a ground of justification.[248] Obviously not all of these grounds of justification would be relevant for data protection.[249] As will be shown, the defence of consent is particularly apposite, as well as performance in a statutory or official capacity and the basic principles underlying necessity, private defence, privilege, and fair comment.[250]

Because the existing grounds of justification are not a *numerus clausus*, it is not essential for data processing to meet the requirements of any of the traditional grounds – as long as the conduct is not *contra bonos mores* there is no wrongfulness.[251]

245 Burchell *Delict* 67; Neethling, Potgieter & Visser *Delict* 76; Van der Walt & Midgley *Delict* 95 (par 78).

246 Neethling, Potgieter & Visser *Delict* 77; Van der Merwe & Olivier *Onregmatige daad* 70 *et seq*; Van der Walt & Midgley *Delict* 95 (par 78).

247 Neethling, Potgieter & Visser *Delict* 342; Van der Merwe & Olivier *Onregmatige daad* 407 *et seq*; Van der Walt & Midgley *Delict* 96 (par 78). See as to reasonable publication, *National Media Ltd v Bogoshi* 1998 4 SA 1196 (SCA); *Khumalo v Holomisa* 2002 5 SA 401 (CC); Neethling 2002 *SALJ* 700 *et seq*.

248 Neethling *Persoonlikheidsreg* 315; Burchel *Personality rights* 272–275 .

249 Defences not discussed include provocation and power to discipline.

250 In the case of defamation the defence is actually truth and public interest, but since privacy is invaded by the publication of true private facts, the truth of the infringing publication cannot be a defence. See below par b.v.

251 Neethling *Persoonlikheidsreg* 330 fn 82; Van der Mewe and Olivier *Onregmatige daad* 70.

b Traditional grounds of justification for infringement of privacy and identity

i Consent

Where a person who is legally capable of expressing his or her will, freely and lawfully gives his or her consent to specific conduct, the harm that ensues from such conduct will be justified and therefore lawful.[252] This idea is expressed in the maxim *volenti non fit injuria*.[253] The maxim is also applied to cases where a person has consented to run the risk of unintentional harm, for example as a participant in a sports match.[254]

It is evident from the comparative research that the consent of the data subject is an important ground that justifies the processing of personal data.[255] Consent is especially relevant when infringement of privacy is involved, in other words when true personal facts are processed. This is so because the individual determines what he or she considers to be private and "absent a will to keep a fact private, absent an interest (or right) that can be protected".[256] However, consent is also relevant when the right to identity is infringed (in other words when false or misleading data are processed) because where a person has consented to his or her personality being misrepresented, the principle *volenti non fit iniuria* applies.[257]

252 Boberg *Delict* 724; Neethling, Potgieter & Visser *Delict* 97; Van der Merwe & Olivier *Onregmatige daad* 89; Van der Walt & Midgley *Delict* 113 (par 89).

253 Boberg *Delict* 724; McKerron *Delict* 67; Neethling, Potgieter & Visser *Delict* 98; Van der Merwe & Olivier *Onregmatige daad* 89; Van der Walt & Midgley *Delict* 112 (par 89).

254 McKerron *Delict* 67; Neethling, Potgieter & Visser *Delict* 97; Van der Merwe & Olivier *Onregmatige daad* 89 96. Consent to the risk of injury should not be confused with contributory intent (or contributory negligence), sometimes loosely referred to as voluntary assumption of risk (see further Neethling, Potgieter & Visser *Delict* 97). Also see Boberg *Delict* 724 *et seq*.

255 In all of the countries studied, "consent" is an important ground on which processing could lawfully take place (see ch 2 par 4.2.2.4; ch 3 par 4.2.4.2; ch 4 par 4.3.4.2.b.ii and ch 5 par 4.3.4.1.b.i.)

256 *National Media Ltd v Jooste* 1996 3 SA 262 (A) 271.

257 In fact, consent is probably the only valid ground of justification in an "appropriation" case (see Neethling (continued...)

Consent to injury is a unilateral act and therefore need not necessarily be made known to the defendant.[258] However, in the case of data processing it is generally required that the consent should be signified in some way. When sensitive data are processed, written consent is required.[259] Because consent is a unilateral act, it may be unilaterally revoked by the consenting party at any stage preceding the defendant's conduct.[260] An irrevocable consent to invasion of privacy or identity is considered to be *contra bonos mores* and as such invalid.[261] It follows that it should not be acceptable to give consent to unlimited data processing.

Consent is furthermore a legal act which restricts the data subject's rights. To qualify as a legal act it must be apparent or be brought to light.[262] Consent can be given expressly or tacitly (for example by conduct). However, mere acquiescence does not necessarily amount to consent.[263] Data controllers should therefore not be allowed to infer consent from a failure to respond to a communication, for example from a customer's failure to return or respond to a leaflet.

Consent must be given before the prejudicial conduct (the data processing) and as a rule the person

257(...continued)
Persoonlikheidsreg 314). Also see McQuoid-Mason *Privacy* 231 232.

258 Boberg *Delict* 724; Neethling, Potgieter & Visser *Delict* 99; Van der Merwe & Olivier *Onregmatige daad* 90; Van der Walt & Midgley *Delict* 113 (par 89).

259 See ch 3 par 4.2.4.2, 4.2.4.3; ch 4 par 4.3.4.2.b.ii and ch 5 par 4.3.4.1.b.i.

260 Neethling, Potgieter & Visser *Delict* 99; Van der Walt & Midgley *Delict* 113 (par 89); Van der Merwe & Olivier *Onregmatige daad* 89-90.

261 *Jooste v National Media Ltd* 1994 2 SA 634 (C) 647; Neethling *Persoonlikheidsreg* 274–275. Also see Schulze 1994 *THRHR* 75, 80. Schulze discusses a standard waiver clause contained in all applications for life insurance underwritten by members of the Life Office Association of SA. He concludes (81) that this clause is invalid, *inter alia* because it purports to act as an irrevocable consent to the invasion of the privacy of the applicant.

262 Neethling, Potgieter & Visser *Delict* 99. This corresponds with the requirement of the Directive that the consent must be unambiguous. See ch 3 par 2.4.2.4.

263 Neethling, Potgieter & Visser *Delict* 100.

must consent himself or herself.[264] Whether consent has been given in a specific case is a question of fact which has to be proved.[265]

The requirements for a valid consent are also applicable to data processing. Consent is first of all only valid if it was given voluntarily and does not amount to submission.[266] It can for example be argued that consent to the processing of data is invalid if it is set as a condition of employment, or the continuance of a contract of employment, by an employer.[267] The person consenting (the data subject) must furthermore have full knowledge of the extent of the possible harm. The consenting party must also fully appreciate the nature and extent of the harm. A data subject can therefore not validly consent to the processing of personal data if he or she is not given all the necessary information on why personal data have to be processed, what they will be used for, who will have access to them and so on. As stated previously, this information must be given to the data subject before the collection of data takes place.[268] The person must also subjectively consent to the harm.[269] Finally, the consent must be permitted by the legal order, in other words it should not be *contra bonos mores* and the impairment must fall within the limits of the consent.[270]

From the comparative research, it is evident that the unambiguous consent of the data subject is

264 Neethling, Potgieter & Visser *Delict* 100; Van der Walt & Midgley *Delict* 113 (par 89); Van der Merwe & Olivier *Onregmatige daad* 93.

265 Neethling, Potgieter & Visser *Delict* 100;Van der Walt & Midgley *Delict* 113 (par 89); Van der Merwe & Olivier *Onregmatige daad* 90.

266 Burchell *Delict* 68; Van der Walt & Midgley *Delict* 115 (par 89); Van der Merwe & Olivier *Onregmatige daad* 90.

267 Neethling *Persoonlikheidsreg* 329–330.

268 See eg ch 4 par 4.3.4.2. This notion corresponds to the data protection principle of openness or transparency (see ch 6 par 2.2.7).

269 The courts' formulation of consent if it is to be a valid ground of justification, is that the injured party must have "knowledge, appreciation and consent" concerning the injury to which consent is being given (see *Waring & Gillow Ltd v Sherborne* 1904 TS 340, 344). Also see Neethling, Potgieter & Visser *Delict* 102; Schulze 1994 *THRHR* 75, 79; Van der Walt & Midgley *Delict* 114 (par 89).

270 Neethling, Potgieter & Visser *Delict* 103; Van der Walt & Midgley *Delict* 115 (par 89); Van der Merwe & Olivier *Onregmatige daad* 92–93.

recognised as a ground justifying the processing of personal data.[271] The fact that processing of personal data is necessary for the performance of a contract to which the data subject is party (or to complete a precontractual stage at the request of the data subject)[272] is also recognised as a valid ground for data processing. This means that the implied consent of the data subject is accepted in these circumstances.

In the direct marketing context, the issue of consent arises in the form of the question whether consent should be an "opt in" or an "opt out" option for the consumer.[273] The EU Directive on data protection requires that data subjects must have the right to object to the processing of personal data for direct marketing purposes. However, the mechanism is not prescribed. With an "opt in" system, the data subjects must specifically be asked whether they want to be included in a mailing list before their data may be processed lawfully. With an "opt out" system, the data subjects should object if they want their names to be removed from a direct marketing list.[274]

It should be kept in mind that if a data subject does not consent to the processing of his or her data, a data controller may nevertheless be able to lawfully process such data as long as another ground of justification is present. The consent of the data subject should never be the only legitimate ground for the processing of personal data. Consent is merely one practical example of a situation where the *boni mores* would not consider the conduct complained of to be wrongful. As stated previously, the determination of wrongfulness entails a weighing of interests, and if a data controller has a legitimate interest that is being served by the processing of personal data and that interest weighs more heavily than the right to privacy or identity of the individual, the processing would be lawful, despite the fact that the data subject did not consent to such processing. It is therefore not an option, and in fact it would

271 See eg Dir 95/46/EC a 7(a) (see ch 3 par 4.2.4.2).

272 See eg Dir 95/46/EC a 7(b) (see ch 3 par 4.2.4.2).

273 See ch 3 par 4.2.4.7.

274 The Dutch WBP uses an "opt out" system, ie data subjects should register their objections if they do not want to be subjected to direct marketing. The Dutch legislator decided to put the burden on the data subjects to object, because a system where the responsible parties first have to ask the data subjects whether they could be included in processing for direct marketing purposes would have been too burdensome for the data controllers from a financial point of view (WBP *Memorie van toelichting* 168). See ch 5 par 4.3.8.3.

be against public policy, to provide a data subject with a right to "opt out" of all data processing activities.

ii Necessity

Necessity is present when a person, by *vis major*, is put in such a position that he or she can protect his or her legitimate interests, or those of another, only by reasonably violating the interests (such as the privacy or identity) of an innocent third party.[275]

Infringement of the right to privacy would, for example, be justified by necessity where a father publishes information about his missing son who has amnesia, in the hope of finding him.[276] Neethling indicates that a person may also violate the privacy of others to protect his or her commercial interests.[277]

Infringement of the right to identity can be justified by necessity as ground of justification only in highly exceptional circumstances, and then only if it is a situation where false facts are disclosed.[278] Neethling argues that as far as data processing is concerned, only an infringement of privacy, in other words the processing of true private facts, can be justified by necessity. The processing of incorrect or misleading data, which infringes the right to identity, should in principle always be wrongful and never be justifiable.[279]

---

275 Neethling, Potgieter & Visser *Delict* 86–87; Van der Walt & Midgley *Delict* 97 (par 80); Van der Merwe & Olivier *Onregmatige daad* 81.

276 Neethling *Persoonlikheidsreg* 289. Also see McQuoid-Mason *Privacy* 233.

277 For examples of this, see below the discussion of the defence of legitimate private interests.

278 Coetser *Identiteit* 216; Neethling *Persoonlikheidsreg* 314. Coetser *Identiteit* 217 gives the example of a doctor who does not want to give the correct information regarding a terminally ill patient to the patient or his or her family, because he or she fears that the news will give the patient a physical or mental setback. The doctor can rely on necessity to justify the fact that he or she has given a misrepresentation of the patient's true physical condition, because it is the only way in which the patient's physical or mental integrity can be protected.

279 Neethling "Databeskerming" 117; *Persoonlikheidsreg* 330.

The following important principles should be borne in mind in evaluating the defence of necessity: A person may inflict harm in a situation of necessity only if the danger existed or was imminent and he or she has no other reasonable means of averting the danger;[280] one may not rely on necessity if one is legally obliged to endure the danger;[281] the means used and measures taken to avert the danger of harm must, in the light of all the circumstances, not be excessive and the principle of proportionality (or commensurability) should always be applied in that the interest that is protected should be of equal or more value than the interest sacrificed.[282]

The underlying principles of this defence should be applied in order to evaluate the lawfulness of data processing based on the need to protect legitimate private interests.[283] For example, no more data should be processed than is necessary for a lawful purpose.[284]

iii Private defence

Private defence is present when a person defends himself or herself against another's actual or imminently threatening wrongful act in order to protect his or her own legally recognised interests or the legally recognised interests of someone else.[285] Acts of private defence that justify an infringement of privacy seldom occur[286] and are difficult to imagine in the context of data processing. Private defence may come into play in highly exceptional circumstances where the right to identity is infringed, but it can only apply in a case of publication of false information; as suggested above, it cannot be used to justify

280 Burchell *Delict* 75; Neethling, Potgieter & Visser *Delict* 89 90; Van der Walt & Midgley *Delict* 98 (par 80).

281 Neethling, Potgieter & Visser *Delict* 90; Van der Walt & Midgley *Delict* 98 (par 80).

282 Neethling, Potgieter & Visser *Delict* 90; Van der Merwe & Olivier *Onregmatige daad* 82–83; Van der Walt & Midgley *Delict* 98 (par 80).

283 See par c.i below.

284 This embodies the data protection principle of minimality (ch 6 par 2.2.3.)

285 Boberg *Delict* 787–788; Burchell *Delict* 74; Neethling, Potgieter & Visser *Delict* 77; Van der Walt & Midgley *Delict* 99 (par 81).

286 Neethling *Persoonlikheidsreg* 290.

the processing of false information.[287] Since this defence is not relevant for data protection, it is not discussed any further. This does not mean that the underlying principles of this defence cannot be applied in order to evaluate the lawfulness of data processing based on the need to protect legitimate private interests. This will be discussed in more detail below.[288]

iv Statutory authority, official capacity and public interest

The defence of statutory authority means that a person has not acted wrongfully if he or she performs an act which would otherwise have been wrongful, while exercising a statutory authority. Harmful conduct authorised by statute or by law in general is thus reasonable and justified and consequently lawful.[289] Data processing by the state is usually done on the basis of statutory authority.[290]

Two underlying principles of this defence are that the statute in question must authorise the infringement of the interest concerned, and that the conduct must not exceed the bounds of the authority conferred by the statute.[291] Whether the statute invoked by the defendant really excuses the otherwise wrongful

287 Neethling *Persoonlikheidsreg* 314.

288 See par c.i below.

289 *Union Government (Minister of Railways) v Sykes* 1913 AD 156 169; *Johannesburg Municipality v African Realty Trust Ltd* 1927 AD 163; *Minister of Community Development v Koch* 1991 3 SA 751 (A); *Government of the Republic of South Africa v Basdeo* 1996 1 SA 355 (A); Boberg *Delict* 771; Neethling, Potgieter & Visser *Delict* 105. Privacy is constitutionally protected, and as such any statute infringing on it must meet the requirements of the limitations clause of the Constitution, 1996 s 36. According to s 36(1) the rights in the Bill of Rights may be limited only in terms of law of general application to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom, taking into account all relevant factors including: (a) the nature of the right, (b) the importance of the purpose of the limitation, (c) the nature and extent of the limitation, (d) the relation between the limitation and its purpose and (e) less restrictive means to achieve the purpose.

290 *S v Bailey* 1981 4 SA 187 (N) (see ch 8 par 2). Acts that allow the state to process personal data in South Africa include, eg, the Statistics Act 6 of 1999; the Income Tax Act 72 of 1986, the Identification Act 68 of 1997; and the Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002. This last mentioned Act, which will replace the Interception and Monitoring Prohibition Act 127 of 1992, requires (s 30) of service providers to provide a telecommunication service which has the capability to be intercepted and to store communication-related information. See also ch 1 par 1.3.

291 *Johannesburg Municipality v African Realty Trust Ltd* 1927 AD 163 172; *Sambo v Milns* 1973 4 SA 312 (continued...)

conduct depends upon the intention of the legislature.[292] The intention of the legislature must be determined by interpreting the statute authorising the infringement.[293] If the plaintiff wants to show that the authorised act exceeded the bounds of the authority, he or she must prove that it was possible for the defendant to have exercised the powers without infringing the plaintiff's interests or that it was possible for the defendant to have prevented or minimised the damage by taking reasonable precautions or by using another method of execution.[294]

If a person in a public office is authorised by common law or by statute to perform certain acts, the person will not be acting wrongfully if he or she injures another in the exercise of his or her duties. This defence is especially relevant in the case of judicial officers and law enforcement officers.[295] However, the particular conduct must still be reasonable and must not fall outside the limits of their jurisdiction. The fact that the person acting in an official capacity acted with malice would be a strong indication, for example, that the person exceeded the bounds of the defence.[296]

What these two traditional grounds of justification, namely statutory authority and official capacity, have in common is that they both serve to protect the public interest in areas such as the prevention of crime,

291(...continued)
(T) 320; McKerron *Delict* 75; Neethling, Potgieter & Visser *Delict* 105; Van der Merwe & Olivier *Onregmatige daad* 104; Van der Walt & Midgley *Delict* 2 (par1).

292 *Johannesburg Municipality v African Realty Trust Ltd* 1927 AD 163; Boberg *Delict* 771; Neethling, Potgieter & Visser *Delict* 105; Van der Merwe & Olivier *Onregmatige daad* 104; Van der Walt & Midgley *Delict* 102 (par 82).

293 For the guidelines applied by the courts in this regard, see Neethling, Potgieter & Visser *Delict* 106; Van der Merwe & Olivier *Onregmatige daad* 104–105; Van der Walt & Midgley *Delict* 101–102 (par 82).

294 Neethling, Potgieter & Visser *Delict* 106; Van der Merwe & Olivier *Onregmatige daad* 105; Van der Walt & Midgley *Delict* 102 (par 82).

295 Neethling, Potgieter & Visser *Delict* 107; Van der Merwe & Olivier *Onregmatige daad* 106; Van der Walt & Midgley *Delict* 108 (par 85).

296 Neethling, Potgieter & Visser *Delict* 107; Van der Merwe & Olivier *Onregmatige daad* 106; Van der Walt & Midgley *Delict* 108 (par 85).

the upholding of law and order, state security, public health, morality and welfare.[297] Public interest can, therefore, be singled out as a ground on which data processing can take place legitimately without infringing the right to privacy. This ground of justification will be discussed in more detail below.[298]

v Impossibility

The concept "impossibility" may play a role in excluding liability when applied to different elements of a delict – conduct, wrongfulness and fault.[299] In the data processing context, impossibility is relevant as a ground of justification that excludes wrongfulness.

If it is impossible for a data controller to comply with a data protection principle, even though it did everything reasonably (in other words, like a reasonable data controller in that particular branch of the data industry) possible to ensure compliance with the principle in question, the data controller should have a valid defence against any claim for non-compliance with that principle.[300] One is not concerned here with physical impossibility, but impossibility according to the legal convictions of the community,[301] that is, the convictions of society regarding what could reasonably be expected from the data controller in question – thus an application of the *boni mores* criterion.[302] If the controller acted reasonably in this sense, wrongfulness is excluded.

vi Defences in defamation cases

Privilege (or privileged occasion) and fair comment, defences traditionally used in defamation cases,

297 See Neethling 1971 *THRHR* 243, 245; Neethling, Potgieter & Visser *Neethling's Law of personality* 266.

298 See par c.i below.

299 Neethling, Potgieter & Visser *Delict* 92.

300 Neethling *Persoonlikheidsreg* 316, 336.

301 See eg *Regal v African Superslate* 1963 1 SA 102 (A). See further Neethling, Potgieter & Visser *Delict* 92.

302 Neethling *Persoonlikheidsreg* 316, 336.

can also justify an infringement of the right to privacy,[303] and in exceptional cases, also of the right to identity.[304]

But the defence of truth and public interest is not applicable to privacy infringement, since this defence requires that the facts published should be true while privacy can only be infringed by the publication of true information. However, the fact that the publication of private information was in the public interest should be a valid defence on its own, and merits further discussion.[305]

Identity is infringed only when untrue information is published. The defences of truth and public interest and fair comment can therefore not justify an infringement of identity, since both require that the published facts should be true.[306] Again, public interest alone may be a good defence in very limited circumstances.[307]

❒ Privileged occasion

A distinction is made between absolute and relative privilege. In the case of absolute privilege the defendant is protected absolutely against liability. These instances are regulated by statute and include the freedom of speech given to members of parliament during proceedings in parliament.[308] Since this defence is not relevant for data processing, it is not discussed any further.

303 *Jansen van Vuuren v Kruger* 1993 4 SA 842 (A) 850; Neethling*Persoonlikheidsreg* 302; McQuoid- Mason *Privacy* 218.

304 Neethling *Persoonlikheidsreg* 315; Coetser *Identiteit* 233. Privileged occasion can be raised as a defence in respect of any claim under the *actio iniuriarum* (Van der Walt & Midgley *Delict* 121 (par 92); *Jansen van Vuuren v Kruger* 1993 4 SA 842 (A)).

305 See below par c.i below.

306 See Neethling *Persoonlikheidsreg* 315.

307 See Neethling *Persoonlikheidsreg* 315–316.

308 See s 58(1) and 71(1) of the Constitution, 1996; Neethling, Potgieter & Visser *Delict* 343. Van der Walt & Midgley *Delict* 121 (par 92) are of the opinion that absolute privilege is not a defence against wrongfulness, but that those who are said to have absolute privilege have in fact immunity from suit.

Relative privilege[309] is applicable *inter alia* to comments made in order to discharge a legal, moral or social duty or in the furtherance of a legitimate interest.[310] For this defence to justify an infringement of privacy, a person must have a social, moral or legal duty or interest to reveal private information about someone and the person or people receiving the private information must have a reciprocal duty or legitimate interest in receiving such information.[311] Moreover, the information must be relevant to the interest being served or reasonably connected to it.[312] The defence of privilege exists for a specific purpose and the facts revealed by the defendant must be relevant to that purpose.[313] The question of relevance is evaluated objectively according to the reasonable person criterion.[314]

An example of an instance where this defence will justify an infringement of privacy is where a person's former employer supplies personal information concerning the employee to a prospective employer, or where a teacher reveals confidential facts about a student to the student's parents.[315]

In the case of infringement of identity, the facts that are revealed are false or incorrect. The defence of privilege can also justify the publication of false facts about someone, provided that there were reasonable grounds present that would have convinced a reasonable person that the facts were true and relevant,[316]or that special circumstances were present, such as the urgency of the situation[317] which

309 See eg *Nydoo v Vengtas* 1965 1 SA 1 (A) 21; *Jordaan v Van Biljon* 1962 1 SA 286 (A) 295–296; Neethling, Potgieter & Visser *Delict* 344. Relative privilege also exists for statements made during judicial or quasi-judicial proceedings, as well as for reports on such proceedings (Neethling, Potgieter & Visser *Delict* 344; Van der Walt & Midgley *Delict* 122 (par 92); Van der Merwe & Olivier *Onregmatige daad* 417 *et seq*).

310 McKerron *Delict* 189 192; Neethling, Potgieter & Visser *Delict* 343; Van der Walt & Midgley *Delict* 122 (par 92); Van der Merwe & Olivier *Onregmatige daad* 409 *et seq*.

311 Neethling *Persoonlikheidsreg* 302; Van der Walt & Midgley *Delict* 121–122 (par 92).

312 Neethling "Privaatheid en universiteite" 136.

313 Strauss et al *Mediareg* 284 285.

314 Neethling *Persoonlikheidsreg* 179.

315 Neethling *Persoonlikheidsreg* 302.

316 Coetser *Identiteit* 235–236; Neethling *Persoonlikheidsreg* 179–180. Even false statements may therefore be relevant (*Borgin v De Villiers* 1980 3 SA 556 (A) 578–579; *Herselman v Botha* 1994 1 SA 28 (A) 35–36; (continued...)

made checking of facts difficult. It would, for example, probably be reasonable for a credit bureau that received incorrect information from the spouse of a data subject to have assumed that the data were correct.

In the case of relative privilege the defendant enjoys provisional protection only and this protection falls away if the plaintiff proves that the defendant exceeded the bounds of the privileged occasion.[318] Malice, improper motive or the pursuit of an illegitimate purpose will lead to the forfeiture of the defence.[319]

❒ Fair comment

This defence is based on the idea that everyone has the right to express an opinion honestly and fairly on matters of public interest and is "an essential part of the greater right of free speech".[320]
In order to justify an invasion of privacy, the comment must be on personal facts that are true and in the public interest.[321] Malice or improper motive will also lead to the forfeiture of this defence.[322]

Where, for example, a teacher is asked for a letter of reference on a student, and the teacher makes comments (positive or negative) on his or her personal information, such disclosure of personal information would be justified by this defence.

316(...continued)
Neethling, Potgieter & Visser *Delict* 344 fn 158). Note that a judicial officer cannot exceed the bounds of this defence because of lack of relevance (*May v Udwin* 1981 1 SA (A) 19–20).

317 Coetser *Identiteit* 235

318 Neethling *Persoonlikheidsreg* 175; Neethling, Potgieter & Visser *Delict* 343; Van der Merwe & Olivier *Onregmatige daad* 407.

319 Van der Walt & Midgley *Delict* 122 (par 92).

320 *Kemsley v Foot* [1950] 1 All ER 331 (CA) at 338 quoted in McKerron *Delict* 200.

321 McKerron *Delict* 203; Neethling, Potgieter & Visser *Neethling's Law of personality* 169; Van der Walt & Midgley *Delict* 123 (par 93).

322 Neethling, Potgieter & Visser *Neethling's Law of personality* 170; Van der Walt & Midgley *Delict* 123 (par 93).

c Newly formulated grounds for lawful processing of personal data

From the comparative research, it is evident that the following further grounds are in general considered to be valid grounds for justifying data processing, namely the fact that the processing is necessary –

- for compliance with a legal obligation to which the controller is subject[323]
- in order to protect the vital interests of the data subject[324]
- for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed[325]
- for the legitimate interests of the controller or third parties to whom the data are disclosed, except where such interests are overridden by the data subject's interests in his or her right to privacy and identity[326]

These grounds can be summarised as the maintenance and furtherance of a legitimate private interest[327] or of the public interest.[328]

---

323 See eg Dir 95/46/EC a 7(c) (see ch 3 par 4.2.4.2).

324 See eg Dir 95/46/EC a 7(d). "Vital interest" is described in the recitals par (31) of Dir 95/46/EC as "an interest which is essential for the data subject's life" (see ch 3 par 4.2.4.2).

325 See eg Dir 95/46/EC a 7(e) (see ch 3 par 4.2.4.2). Examples would eg be a task carried out in the public interest or in the exercise of official authority by a public administration or another natural or juristic person governed by public law, or by private law as in the case of a professional association (see Dir 95/46/EC recitals par (32)).

326 Dir 95/46/EC a 7(f) (see ch 3 par 4.2.4.2).

327 The protection of the vital interests of the data subject or the legitimate interests of the controller or third parties is considered to be part of this ground.

328 Depending on the circumstances, the necessity of complying with a legal obligation may be regarded as part of the private interest or public interest ground.

i Maintenance and furtherance of legitimate private interests

The processing of personal data by private persons or institutions (data controllers[329]) can be justified on the ground of the furtherance of a legitimate private interest.[330] Neethling supports this ground of justification and emphasises that it is not based on a new idea, because, he argues, the concept of "maintenance of legitimate interests" can only mean that where it is necessary to protect his or her legitimate interests, the defendant may do so.[331] Neethling continues: "Viewed thus, this ground of justification is closely connected to, for example, private defence and necessity, because the same line of thought forms their basis."[332]

The principles underlying necessity and private defence should therefore be taken into account when establishing the boundaries of the defence of maintenance and furtherance of legitimate private interests. These principles require, for example, that effect should be given to the principle of proportionality. When determining the lawfulness or otherwise of the processing of personal data, the interest furthered by the processing should therefore be balanced against the data subject's right to privacy, and the interest that weighs the most heavily, should be upheld.[333] In this process all relevant facts and surrounding circumstances must be taken into consideration.

The most prominent private interests that are protected by the processing of data are private

329 Typical examples of data controllers in the private sphere are credit bureaux, banks, direct marketing agents, employers, the insurance industry, medical professionals and voluntary associations such as clubs, churches and political parties (also see ch 1 par 1.4).

330 See also WBP a 8(e) (ch 5 par 4.3.4.1).

331 Neethling *Persoonlikheidsreg* 288–289.

332 Neethling, Potgieter & Visser *Neethling's Law of personality* 263; Neethling *Persoonlikheidsreg* 289. Van der Walt & Midgley *Delict* 103 (par 83) are of the opinion that under the new constitutional dispensation, the defence that a plaintiff's rights have been infringed while the defendant has been exercising a recognised right will in future gain prominence in South African law. It is suggested that the latter is similar to saying that a legitimate interest has been maintained.

333 Neethling *Privaatheid* 74. All the countries studied also recognise that processing of personal data may take place lawfully where the processor has a legitimate interest in doing so (see eg ch 3 par 4.2.4.2.vii; ch 4 par 4.3.4.2.b.ii; ch 5 par 4.3.4.1.b.vii).

commercial interests. Employers may, for example, obtain information about prospective employees, because employers have a legitimate interest in appointing reliable and honest employees.[334] Similarly, to protect their commercial interests, insurers may obtain information about the risk posed by their prospective clients, or financial institutions about the creditworthiness of such clients.[335]

Because it is impracticable for individuals or institutions (such as potential employers, insurers, sellers, lessors and financiers) to obtain reasonably sufficient information regarding particular individuals themselves, it is seen as reasonable that the task should be performed by institutions (such as credit bureaus) which possess the necessary means and efficiency to process complete data records on a permanent basis. The latter institutions then make the information in their possession available to interested parties.[336]

Neethling[337] enumerates the following requirements that must be satisfied if the processing of data is to be deemed lawful on the ground of protecting legitimate commercial interests:

- It should first of all be determined objectively that the interest which the person (data controller) wants to maintain by invading the privacy of another party through data processing is a legitimate interest worthy of protection. This must be determined with reference to the *boni mores* criterion for wrongfulness.[338] Interests recognised at common law or in the Constitution as worthy of protection, such as freedom of expression, freedom of religion, belief and opinion, freedom of association, political rights, the freedom to choose a trade, occupation or profession and the right to have access to information, are examples of legitimate interests.[339] If the interest

334 Neethling *Persoonlikheidsreg* 289.

335 Neethling *Persoonlikheidsreg* 290. On creditworthiness, see par 2.1 above.

336 Neethling *Persoonlikheidsreg* 330; "Databeskerming" 117.

337 Neethling *Persoonlikheidsreg* 330.

338 See par 2.3.2.2 above.

339 Act 108 of 1996 ss 16, 17, 18, 19, 22, 32.

is not recognised by law and is therefore not a legitimate one, the processing will be wrongful, unless another ground of justification is present, such as consent of the data subject.[340] In situations where two or more fundamental rights are in conflict, such as the right to privacy and the right to freedom of trade, occupation and profession, there must be a fair weighing up or balancing of the opposing rights.[341]

❒ The same principle underlies the view that data may be processed only for one or more specified lawful purposes.[342] Data processing can have a lawful purpose only if the object is to further or protect a legitimate interest and in order that the interests involved may be identified, the purpose must clearly disclose which interest is at stake. The implication here is that the purpose must be clearly defined or circumscribed. Without such definition it would be very difficult to judge whether or not the processing of data is lawful – in other words, whether a legitimate interest is being protected.[343]

❒ It follows from this that the data may be used or communicated only for the protection of the legitimate interests involved and that the use of data in a manner incompatible with this purpose is wrongful.[344] It also follows that there should be a duty of confidentiality on a data controller

340 Neethling *Persoonlikheidsreg* 330. Also see Convention 108/1981 a 5; Dir 95/46/EC a 6(1)(b); DP Act of 1998 sch 1 part I principle 2; WBP a 7.

341 Neethling, Potgieter & Visser *Delict* 21; Neethling *Persoonlikheidsreg* 96.

342 See ch 6 par 2.2.2.

343 Neethling *Persoonlikheidsreg* 330–331. Also see OECD Guidelines par 9; Convention 108/1981 a 5; Dir 95/46/EC a 6(1)(b); DP Act of 1998 sch 1 part I principle 2; WBP a 7. This is a reflection of the data protection principles of fair ad lawful processing and purpose specification (see ch 6 par 2.2.1 and 2.2.2).

344 Also see Convention 108/1981 a 5; Dir 95/46/EC a 6(1)(b); DP Act of 1998 sch 1 part I principle 2; WBP a 7. Neethling *Persoonlikheidsreg* 331 fn 86 points out that this principle is not in conflict with the constitutionally protected right of "anyone to have access to any information that is held by another person and that is required for the exercise or protection of any rights" (s 32(1)(b) of the Constitution, 1996) because the information is given to persons who have a legitimate interest in it. This is also a reflection of the common law defence of privilege as discussed above, since the data may be communicated only to a person who has a legitimate interest in the data (Neethling *Persoonlikheidsreg* 331 fn 86).

not to communicate processed information outside the originally specified purpose.[345]

- A further requirement, related to the previous one, is that unauthorised access to processed data by an outsider in principle constitutes an unlawful intrusion into the privacy of the individual involved, even though the outsider may have a legitimate interest in the data.[346]

- Even if it has been established that the processing is for the protection of a legitimate interest, the processing should nevertheless be carried out in a reasonable manner.[347] A requirement which plays an important role in this regard is that the nature and extent of the compiled data should be reasonably necessary for, and consequently also related to (or relevant to), the protection of the interest - in other words, no more information than is necessary for this purpose should be processed.[348] The defined or specified purpose therefore also circumscribes the limits of data processing.[349]

345 Neethling *Persoonlikheidsreg* 331. This reflects the data protection principle of disclosure limitation (see ch 6 par 2.2.5).

346 Neethling *Persoonlikheidsreg* 331 fn 87. Neethling points out that unauthorised access amounts to self-help that should not be tolerated even if the party has an interest in the information and consequently a right of access to it in terms of s 32(1)(b) of the Constitution. This requirement relates to the security and confidentiality principle of data protection (see ch 6 par 2.2.9).

347 The unreasonable maintenance of an interest, causing damage to someone, is in principle unlawful in our law (see Neethling *Persoonlikheidsreg* 293 fn 180, 331 fn 88; Van Heerden & Neethling *Unlawful competition* 135–137). Compare also *Gosschalk v Rossouw* 1966 2 SA 476 (C) 490–482. Also see fn 174 on the so-called doctrine of "abuse of rights". On "lawful and fair processing", see further ch 6 par 2.2.1.

348 Compare also the defence of privilege discussed above as well as the principle applicable to necessity and private defence, namely that the means used to avert the damage should be necessary and not excessive (above). See also *Gosschalk v Rossouw* 1966 2 SA 476 (K) 490–492. Compare *Le Roux v Direkteur-generaal van Handel en Nywerheid* 1997 4 SA 174 (T) 185 where the court required that the information requested from the state in terms of s 23 of the 1993 Constitution (see fn 344 above) should be "reasonably" required for the exercise of applicant's rights.

349 Neethling *Persoonlikheidsreg* 331. See also Convention 108/1981 a 5; Dir 95/46/EC a 6(1)(b); DP Act of 1998 sch 1 part I principle 3; WBP a 11(1). This reflects the data protection principle of minimality (see ch 6 par 2.2.3).

Neethling *Persoonlikheidsreg* 331–332 uses the activities of credit bureaus as an example. The purpose of these institutions is to process data for the protection of business interests in creditworthiness; thus only data reasonably linked to creditworthiness should be gathered and communicated. Any other personal facts, such as drinking habits, physical or mental health, extramarital affairs, political views and religious affiliation are usually unnecessary for the specified purpose and should therefore not be

(continued...)

❒ An important application of the previous requirement is that obsolete data is generally not reasonably necessary for the protection of a legitimate interest. Therefore data may not be stored or used for longer than is reasonably necessary for the specified purpose.[350]

❒ Furthermore, incorrect (false) or misleading data cannot be necessary for the protection of a legitimate interest. Such data may therefore not be stored or used.[351]

If information which is unnecessary[352] for the protection of a legitimate interest or obsolete, misleading or incorrect information[353] is acquired and communicated, the bounds of justification have been exceeded and such conduct is then unreasonable and thus wrongful. Whether information is reasonably necessary is a factual question which must be determined with reference to all the relevant circumstances of a particular case.[354]

❒ The bounds of reasonableness in relation to protecting a legitimate interest are also exceeded where data which have been obtained in an unlawful manner (such as by reading private documents, illegal wire-tapping or shadowing a person) are processed.[355] Differently stated, on account of the continuing wrongfulness in these instances, such data may not be processed because the processing is inseparably linked to the original wrongfulness. Neethling[356] points out that if the collection and use of this type of information were regarded as lawful, the data

349(...continued)
processed. See also McQuoid-Mason 1982 *CILSA* 135 139.

350 Also see OECD Guidelines par 8; Convention 108/1981 a 5; Dir 95/46/EC a 6(1)(d); DP Act of 1998 sch 1 part I principle 4; WBP a 11(2).This is a reflection of the data protection principle of quality (see ch 6 par 2.2.3).

351 See text to fn 279. Again, this reflects the data protection principle of quality (see ch 6 par 2.2.3).

352 See the minimality principle of data protection (ch 6 par 2.2.3).

353 See the quality principle of data protection (ch 6 par 2.2.4).

354 Neethling *Persoonlikheidsreg* 332.

355 Neethling *Persoonlikheidsreg* 332. See text accompanying fn 202.

356 Neethling *Persoonlikheidsreg* 332.

industry would be tempted to employ illegal methods of obtaining information – a practice which cannot be accepted.

- Finally, the processing of sensitive information is considered unreasonable in principle because of the drastic infringement of privacy (unless otherwise specifically provided for).[357]

ii Maintenance and furtherance of the public interest

The maintenance and furtherance of the public interest may also be held to justify the processing of personal data.[358] Processing may be done by either private persons or the state. In the case of the former, the press, for example, may process data for the maintenance of the public interest in information,[359] or a bank may disclose personal information on a client in order to serve the public interest in preventing crime.[360]

Where the state or a public institution processes personal information to protect the public interest, this ground of justification is usually based on statutory authority.[361] In this regard personal information may be processed in order to uphold law and order, prevent crime and disorder and to promote public

357 Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership and health or sex life of an individual is considered to be sensitive by all the countries studied. Processing of sensitive data is permitted in limited circumstances only (see eg ch 3 par 4.2.4.3). See also the data protection principle of sensitivity (ch 6 par 2.2.8).

358 Also see WBP a 8(e).

359 On the press and the maintenance of the public interest in information, see Neethling *Persoonlikheidsreg* 294. See also ch 3 par 4.2.4.4, ch 4 par 4.3.6.2 and ch 5 par 4.3.3.2 on special provisions regarding data protection and freedom of expression in the comparative study.

360 Meiring *Betalingstelsel* 350–351. However, in order to justify such a breach of a confidential relationship, the public interest in the information would have to be very cogent indeed. Such a public interest is eg present where a doctor reveals the medical condition of a patient to the traffic authorities, because the medical condition of the patient poses a serious threat to the safety of other road users (Neethling *Privaatheid* 77). Similarly, one can argue that a doctor may reveal the fact that a patient is HIV positive to the partner(s) of such a patient, where the doctor knows that the patient has refused to inform his or her partner(s) and is continuing to practice unsafe sexual intercourse.

361 Discussed above.

health, morality and welfare.[362] The state processes a variety of personal data, owing to its numerous activities and functions, *inter alia*, data on civil servants (as employees); members of the armed forces including former conscripts; pupils and students at educational institutions; suspects, accused persons and prisoners; taxpayers; welfare recipients; patients in state hospitals; and all individuals in terms of census reports and registration of the population.[363] The processing of this information is essential for the proper functioning of the state administration and for effective state planning.[364] Individuals are also sometimes compelled by legislation to furnish the information. In some cases this information is processed anonymously in statistical format, but in other instances, such as for the detection of crime, the information must of necessity refer to a particular individual.

In order to evaluate the lawfulness of a processing of personal data based on the public interest, it would be necessary to refer to the statute authorising the processing.[365] The constitutional dispensation should of course also be taken into account. In the South African context, where the Constitution recognises the right to personal privacy as a fundamental human right,[366] any legislation permitting data processing which infringes on a person's right to privacy would have to be tested against the criteria provided by the Constitution for the validity of statutes limiting fundamental rights.[367] As stated previously, where two or more fundamental rights are in conflict there must be a weighing up or

362 Neethling *Persoonlikheidsreg* 332. Privacy is constitutionally recognised as a fundamental right; consequently any legislation limiting the right to privacy must meet the requirements of the limitation clause of the Constitution (s 36) (see fn 120, 289).

363 See also ch 1 par 1.4.

364 See *S v Bailey* 1981 4 SA 187 (N) 190 (see ch 8 par 2.2); Neethling *Persoonlikheidsreg* 324.

365 Neethling *Persoonlikheidsreg* 332; Burchell *Delict* 79 *et seq*.

366 Constitution, 1996 s 14.

367 Generally the state and its organs will be allowed to obtain, store and use personal information only if this action is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom (see Constitution, 1996 s 36). Moreover, the interests of an individual are safeguarded to a certain extent in that or he or she has access to all information (including information regarding himself or herself) held by the state or any of its organs in terms of the Promotion of Access to Information Act 2 of 2000. See further ch 8 par 4.2.

balancing of the opposing rights.[368]

In order for the collection and processing of data to be lawful in this context, certain general requirements must be met, most of which are analogous to the requirements which apply in the case of the maintenance of legitimate private interests as discussed above. Neethling[369] enumerates the following:

- The state must be expressly authorised by a valid statutory provision to process data.[370] In order to be valid, the statutory provision must comply with constitutional requirements.

- The data processing must be done only for the purposes recognised by the statutory authorisation.[371]

- The protection of the public interest must take place in a reasonable manner, which means that the data used in the data processing must be reasonably necessary for and related to the statutory purpose.[372]

- The data may not be processed for longer than is necessary for the statutory purpose.

- Data acquired in an unlawful manner may not be processed.

If the state or its organs exceed their statutory authority, their conduct is wrongful and they may not be

368 Neethling, Potgieter & Visser *Delict* 21; Neethling *Persoonlikheidsreg* 96.

369 Neethling *Persoonlikheisdreg* 333.

370 See above par 2.3.2.3.b.iv. Without an express statutory authorisation, data processing by the state should be regarded as unlawful unless the consent of the individual has been obtained (see Neethling "Databeskerming" 120 fn 104). This principle is further supported by s 14 of the Constitution, 1996 which recognises the right to personal privacy as a fundamental human right.

371 See above par 2.3.2.3.b.iv; see also Van Wyk 1996 *THRHR* 626, 633.

372 See par 2.3.2.3 above where this issue is discussed in relation to the protection of private interests.

allowed to make use of the fruits of such illegality.

Neethling also emphasises that if any data controller (private or public) collects and communicates personal information for statistical purposes, it should take steps to ensure anonymity; in other words, the statistics should not be identified with a particular individual. If this requirement is not met, the data controller is acting unlawfully because the processing is not reconcilable with the specified purpose, namely data processing in order to generate impersonal statistics.[373]

2.3.3 Fault

2.3.3.1 Nature of fault and accountability

Once the wrongfulness of a defendant's conduct has been established, the issue of fault arises. Fault is the subjective element of a delict, because it involves a juridical evaluation of the blameworthiness of the defendant.[374] It has been described as that element of delict which induces the law to impute someone's wrongful conduct to that person in the sense of holding him or her legally responsible for it.[375] However, the law will only hold persons accountable for their conduct if they have the ability to make rational judgments and control their conduct accordingly. Persons who lack this ability because of their youth, mental disability, intoxication or the use of drugs are not accountable and are therefore incapable of fault.[376]

2.3.3.2 Forms of fault

373 Neethling *Persoonlikheidsreg* 333 fn 102. Also see the data protection principle of purpose specification (ch 6 par 2.2.2) where the use of personal data for statistical purposes is also referred to.

374 Neethling, Potgieter & Visser *Delict* 119; Van der Walt & Midgley *Delict* 125 (par 95); Van Aswegen *Sameloop* 149.

375 Boberg *Delict* 268.

376 Boberg *Delict* 268; Neethling, Potgieter & Visser *Delict* 120; Van der Merwe & Olivier *Onregmatige daad* 112; Van der Walt & Midgley *Delict* 125 (par 96); Van Aswegen *Sameloop* 150.

Two forms of fault are distinguished, namely intent (*dolus*, *animus iniuriandi*) and negligence. As the law stands at present, in principle the data subject has to prove that the infringement of his or her right to privacy or identity was intentional in order to be successful with the *actio iniuriarum* for *solatium*.[377] Negligence is sufficient for the *actio legis Aquiliae* with which patrimonial loss resulting from the infringement of the personality can be recovered.[378]

a Intent

Fault in the form of intent is a state of mind where the will is directed at producing a particular consequence which the actor knows to be wrongful.[379] The actor's intention, as far as the direction of will is concerned, can take three forms, namely *dolus directus*, *dolus indirectus* and *dolus eventualis*. *Dolus directus* is present when the actor directs his or her will to the attainment of a particular consequence; *dolus indirectus* is present when a person acts with the purpose of attaining a particular object, but at the same time actually foresees that another consequence will flow from that conduct – the person then has *dolus indirectus* with regard to the second consequence; *dolus eventualis* is present when a person acts with the purpose of attaining a particular consequence, but subjectively realises that another consequence may possibly also result from his or her conduct and reconciles himself or herself to this other consequence – the person then has *dolus eventualis* with regard to the possible consequence.[380] For example, if a credit bureau records false information, knowing that it is false, it will have direct intent with regard to infringing the data subject's right to identity. If it records information which it realises may be false, and decides not to check more thoroughly but to take the risk that it is recording false information, it has *dolus eventualis*.

---

377 But see *C v Minister of Correctional Services* 1996 4 SA 292 (T) 304–305 where the state was held strictly liable for infringing the privacy of prisoners. See further fn 438.

378 The remedies for a delict will be discussed in par 2.4.

379 Boberg *Delict* 268; Neethling, Potgieter & Visser *Delict* 123; Van der Merwe & Olivier *Onregmatige daad* 115; Van der Walt & Midgley *Delict* 127 (par 97).

380 Neethling, Potgieter & Visser *Delict* 123–124; Van der Merwe & Olivier *Onregmatige daad* 115–118; Van der Walt & Midgley *Delict* 127 (par 97).

Apart from directing his or her will to causing a particular result, a person must be conscious of wrongfulness before it can be established that the person acted with intent in a juridical sense. This means that the person must have realised or must have foreseen that his or her conduct was wrongful. A mistake on the part of the actor as to any relevant fact or as to the law would therefore exclude his or her intent.[381] If a credit bureau records information which it realises may be false, but thinks that it is justified in recording the information because of the presence of a ground of justification for recording personal information (such as the presence of a statute that instructs it to record personal information) the credit bureau is exceeding the bounds of the ground of justification, but it is not acting with the necessary consciousness of wrongfulness to have intent in a juridical sense.[382]

b Negligence

Fault in the form of negligence is present when an actor does not observe the degree of care which the law requires. The standard of care required in the law of delict is that of the *bonus paterfamilias* (reasonable person). The reasonable person "serves as the legal personification of those qualities which the community expects from its members in their daily contact with one another".[383] The reasonable person is an objective standard,[384] but since the reasonable person is placed in the position of the defendant at the time the delict was committed, the test remains subjective.[385]

Negligence arises if a reasonable person in the position of the defendant would have foreseen the reasonable possibility of his or her conduct causing another person harm, and the reasonable person

381 Neethling, Potgieter & Visser *Delict* 125–126. Also see Van der Merwe & Olivier *Onregmatige daad* 123–126; Van der Walt & Midgley *Delict* 129–130 (par 99).

382 In the area of data processing it is generally very difficult to prove intent on the part of the controller because the controller will usually be able to rely on absence of consciousness of wrongfulness (Neethling 2002 *THRHR* 574, 583). This aspect will be discussed further in par 2.4.

383 Neethling, Potgieter & Visser *Delict* 132.

384 *Weber v Santam Versekeringmaatskappy Bpk* 1983 1 SA (A) 410–411; Neethling, Potgieter & Visser *Delict* 132 fn 75; Van der Walt & Midgley *Delict* 133 (par 101).

385 Van Aswegen *Sameloop* 151–152; Van der Walt & Midgley *Delict* 133–134 (par 101).

would have taken steps to guard against such occurrence, which steps the defendant failed to take.[386] In other words, the test for negligence rests on two pillars, namely the reasonable foreseeability[387] and the reasonable preventability[388] of damage. If a credit bureau collects personal data on data subjects without taking reasonable care to ensure the correctness of such information and then uses such data to the detriment of the data subject, in circumstances where it was reasonable to expect of it to take steps to prevent such harm, it has acted negligently.

2.3.4 Causation

2.3.4.1 Introduction

A wrongdoer can only be held liable in delict if his or her wrongful conduct caused harm.[389] In other words, there must be a causal link between the conduct that produces the damage and the harm

386 *Kruger v Coetzee* 1966 2 SA 428 (A) 430; *Santam Versekeringsmaatskappy Bpk v Swart* 1987 4 SA 816 (A) 819–820; *Ngubane v SA Transport Services* 1991 1 SA 756 (A) 776; *Barnard v Santam Bpk* 1999 1 SA 202 (SCA) 213; *Mkhatswa v Minister of Defence* 2000 1 SA 1004 (SCA) 1111–1112; *Mostert v Cape Town City Council* 2001 1 SA 105 (SCA) 118–119; *Du Pisanie v Rent-a Sign (Pty) Ltd* 2001 2 SA 894 (SCA) 899. But see *Mukheiber v Raath* 1999 3 SA 1065 (SCA) 1077. To put this decision in its correct context, see the discussion by Neethling, Potgieter & Visser *Delict* 138–141.

387 Neethling, Potgieter & Visser *Delict* 137 *et seq*; Van der Walt & Midgley *Delict* 142 *et seq* (par 105); Van der Merwe & Olivier *Onregmatige daad* 128. Two diverging views exist in case law and amongst authors as to the nature of the foreseeability test. On the one hand, there is support for the abstract (or absolute) approach, according to which damage in general must have been foreseeable, and on the other hand, there is also support for the concrete (or relative) approach in terms of which the specific consequence must be reasonably foreseeable. Neethling, Potgieter & Visser *Delict* 139 support the concrete approach, but also point out (140 fn 110) that "because both the concrete and abstract approaches require foreseeability of the general nature of consequence(s) and the general manner in which it occurred ... both approaches should as far as negligence is concerned, produce the same result". It is also important to recognise that in both approaches legal causation should be applied to limit liability (Neethling, Potgieter & Visser *Delict* 140).

388 Once it has been established that a reasonable person would have foreseen the possibility of harm, the question is whether he or she would have taken measures to prevent the occurrence of the foreseeable harm. The answer depends on the circumstances of each case and various factors, (such as the recognisable risk and the social value or utility of the interests served by the defendant's conduct) must be weighed against each other (Van der Walt & Midgley *Delict* 144 (par 105)).

389 "Damage and causation are two separate delictual elements but they have a particular relationship with each other as causation is necessarily determined with reference to a consequence (damage)" (Neethling, Potgieter & Visser *Delict* 218).

suffered.[390] Wrongful data processing can only result in liability for the wrongdoer if a causal link can be proved between the processing of the data and the harm that resulted. Similarly, some demonstrable harm or injury caused by the delict must also be established.[391]

As Van Aswegen[392] points out, the requirement that the harm for which compensation is claimed should have been caused by the conduct of the actor seems so logical that one does not expect it to be problematic. Yet, in Boberg's words, this element is surrounded by "a morass of controversy".[393] According to Boberg, the only two propositions on which there is complete unanimity are that (a) the defendant is not liable unless his or her conduct caused the plaintiff's harm; and (b) the defendant is not liable merely because his or her conduct in fact caused the plaintiff's harm – such liability would be too wide and some means of limiting it must be found.[394]

Causation therefore involves two issues, namely (a) whether a factual relation exists between the defendant's conduct and the harm sustained by the plaintiff (factual causation); and (b) whether and to what extent the defendant should be held legally responsible for the consequences factually caused by him or her (legal causation).[395]

2.3.4.2 Factual causation

The test for factual causation is the first controversial issue. It is submitted that whether a factual causal nexus exists is merely a question of fact (whether one fact flows from the other) that should be

390 See, in general, Boberg *Delict* 380 *et seq*; Neethling, Potgieter & Visser *Delict* 173; Van der Walt & Midgley *Delict* 163 *et seq* (para 111–113); Van der Merwe & Olivier *Onregmatige daad* 196 *et seq*.

391 The element of harm or damage will be discussed in par 2.3.5 below.

392 Van Aswegen *Sameloop* 155.

393 Boberg *Delict* 380.

394 Boberg *Delict* 380.

395 Boberg *Delict* 380 *et seq*, 440 *et seq*; Neethling, Potgieter & Visser *Delict* 173; Van der Walt & Midgley *Delict* 163–164 (par 112).

established in a court of law by way of evidence.[396] However, our courts have accepted the *conditio sine qua non* theory or "but for" test as the applicable test for factual causation.[397] In terms of this test, an act is the cause of the result if the act cannot be thought away without the result also disappearing.[398] In the case of data processing, the plaintiff will therefore have to show that the wrongful processing of personal data by the defendant (controller) (or someone for whom the defendant can be held vicariously liable) was the factual cause of the personality injury and/or patrimonial loss suffered by him or her.

2.3.4.3 Legal causation

If a factual causal link between the data processing and the harm has been established, another thorny issue remains, namely whether the plaintiff should be held liable for causing that damage. Van der Walt and Midgley[399] point out that, as a matter of policy, persons are not called upon to make good all the harm that could be attributed to their wrongful conduct, because the burden would be excessive in some instances; as a matter of policy, a sufficiently close connection should exist before the persons are held liable to compensate others.[400]

In most cases of delict (such as wrongful, intentional or negligent processing of personal data) that causes harm, the harm will clearly fall within the limits of the wrongdoer's liability so that it would be unnecessary to examine legal causation or the imputability of harm in express terms. However, where a whole chain of consecutive or remote consequences results from such data processing, legal causation could become a difficult issue that would have to be dealt with at length.[401]

---

396 See Neethling, Potgieter & Visser *Delict* 182–183.

397 See eg *Minister of Police v Skosana* 1971 1 SA 31 (A); *S v Mokgethi* 1990 1 SA 32 (A); *International Shipping Co (Pty) Ltd v Bentley* 1990 1 SA 680 (A); *Moses v Minister of Safety and Security* 2000 3 SA 106 (C).

398 For criticism of the *conditio sine qua non* theory, see Neethling, Potgieter & Visser *Delict* 176–180.

399 Van der Walt & Midgley *Delict* 168 (par 115).

400 See also Boberg *Delict* 440; Neethling, Potgieter & Visser *Delict* 183–184.

401 Neethling, Potgieter & Visser *Delict* 185.

In the past, different theories for legal causation were formulated and applied by the courts, such as the theories of adequate causation,[402] direct consequences,[403] fault[404] and reasonable foreseeability.[405] The present approach of the courts to legal causation is what is known as a flexible one[406] – there is no single and general criterion for legal causation which is applicable in all instances. In terms of this approach the basic question is whether there is a close enough relationship between the wrongdoer's conduct (the data processing) and its consequence for such consequence to be imputed to the wrongdoer in view of policy considerations based on reasonableness, fairness and justice.[407] With this approach, the existing criteria for legal causation may play a subsidiary role in determining legal causation. As Neethling, Potgieter and Visser explain:[408]

> In terms of the flexible approach, the theories of legal causation are at the service of the imputability question and not *vice versa*. This means that the theories should be regarded as pointers or criteria reflecting legal policy and legal convictions as to when

402 According to this theory a consequence is imputed to a wrongdoer if the consequence is "adequately" connected to the conduct; this would be the case if, according to human experience, in the normal course of events the act has the tendency to bring about that type of consequence (Neethling, Potgieter & Visser *Delict* 190–191). See further Boberg *Delict* 445–447; Van der Walt & Midgley *Delict* 176–177 (par 120); Van der Merwe & Olivier *Onregmatige daad* 204 *et seq*.

403 According to this theory the actor is liable for all the direct consequences of a negligent act. In English law, from which it originates, it was limited to physical consequences and a *novus actus interveniens* could break the causal link (Neethling, Potgieter & Visser *Delict* 192–194). See further Boberg *Delict* 44–442; Van der Walt & Midgley *Delict* 172–173 (par 117); Van der Merwe & Olivier *Onregmatige daad* 202 *et seq*.

404 According to this approach legal causation as an independent element of delict is unnecessary, since the wrongdoer is liable for those consequences in respect of which he was at fault. The supporters of this theory usually apply the concrete approach to negligence (see fn 387). See further Neethling, Potgieter & Visser *Delict* 194–195); Boberg *Delict* 381 *et seq*; Van der Merwe & Olivier *Onregmatige daad* 198 206 *et seq*.

405 Until recently it has been accepted that this criterion, in terms of which the wrongdoer is liable for all the reasonably foreseeable consequences of his wrongful act, is preferred by our courts (Neethling, Potgieter & Visser *Delict* 190–191). See further Boberg *Delict* 445 447; Van der Walt & Midgley *Delict* 168 (par 115); Van der Merwe & Olivier *Onregmatige daad* 216 223–224.

406 See eg *S v Mokgethi* 1990 1 SA 32 (A); *International Shipping Co (Pty) Ltd v Bentley* 1990 1 SA 680 (A); *Smit v Abrahams* 1994 4 SA 1 (A); *Standard Chartered Bank of Canada v Nedperm Bank Ltd* 1994 4 SA 747 (A); *Napier v Collett* 1995 3 SA 140 (A); *Groenewald v Groenewald* 1998 2 SA 1106 (SCA); *Road Accident Fund v Russel* 2001 2 SA 34 (SCA).

407 Neethling, Potgieter & Visser *Delict* 186–189.

408 Neethling, Potgieter & Visser *Delict* 188.

> damage should be imputed to a person: damage is imputable when, depending on the circumstances, it is a direct consequence of the conduct, or reasonably foreseeable, or if it is in an adequate relationship to the conduct, or for a combination of such reasons, or simply for reasons of legal policy.

In case of wrongful, intentional or negligent processing of personal data, the plaintiff must therefore show that there was a sufficiently close nexus between the harm factually caused by the defendant's data processing and the latter's conduct for liability for that loss – with reference to policy considerations based on reasonableness, fairness and justice – to be imputed to the defendant.[409]

2.3.5 Damage[410]

The purpose of the law of delict is to compensate a person for loss suffered;[411] it is therefore a prerequisite for delictual liability that the plaintiff must have suffered harm.[412] However, not all harm is

409 The fact that there was a *novus actus interveniens* or independent event after the defendant's act (data processing) has been concluded, which either caused or contributed to the detrimental consequences for the plaintiff, has to be taken into account in deciding on either factual causation or the reasonability, fairness and justice of imputing the consequences to the defendant (Neethling, Potgieter & Visser *Delict* 205). Another situation that must be considered when legal causation is determined is the situation where a particular plaintiff is an "egg-skull case" (Neethling, Potgieter & Visser *Delict* 207–209). In other words, the plaintiff, because of some physical, psychological or financial weakness, suffered more serious injury or loss as a result of the data processing than would have been the case if the plaintiff had not suffered from such a weakness. It is usually said that "you must take your victim as you find him (or her)" (Van der Walt & Midgley *Delict* 175 (par 119)), implying that a wrongdoer cannot use the fact that the plaintiff was more susceptible to harm as an excuse. However, it is suggested that the most acceptable approach would be to consider the fact that the plaintiff was an "egg-skull" as just one of the relevant facts when deciding whether it is reasonable, fair and just to impute the consequences to the defendant (Neethling, Potgieter & Visser *Delict* 209).

410 Damage should not be confused with damages, which refers to the monetary equivalent of damage awarded to a person in order to eliminate as fully as possible past and future damage (Neethling, Potgieter & Visser *Delict* 236). The assessment of damages (quantification), or the process whereby damage which the law has found to exist and for which compensation may be awarded is expressed in monetary terms in order to reach a specific amount of damages, will not be dealt with. See in general Neethling, Potgieter & Visser *Delict* 237 *et seq*, 253 *et seq*.

411 Neethling, Potgieter & Visser *Delict* 211; Van der Walt & Midgley *Delict* 29–30 (par 31).

412 In the case of the interdict, the plaintiff must show actual or threatened harm (Van der Walt and Midgley *Delict* 29–30 (par 31) fn 1). Note also that "[t]he notion that nominal damages may be awarded in an (continued...)

recognised in law for the purposes of delictual liability – in other words, not all harm is actionable. Sometimes harm has to lie where it falls, or compensation has to be sought on another basis, such as insurance.[413] Only harm in regard to legally recognised patrimonial and non-patrimonial (personality) interests of a person qualifies as damage.[414] From this, it follows that damage can be defined as "the diminution, as a result of a damage-causing event, in the utility or quality of a patrimonial or personality interest in satisfying the legally recognised needs of the person involved."[415]

In the case of data processing, a person first of all suffers an infringement of his or her privacy or identity. There is thus a diminution in the utility or quality of a personality interest of the person involved and therefore harm is suffered. Where the plaintiff claims that the wrongful processing of personal data also caused him or her patrimonial damage, such damage would have to be proved.[416] This does not mean that the plaintiff needs to bring separate actions, because where both patrimonial and non-patrimonial loss arise from a single act, the plaintiff can claim under both heads in a single action.[417]

In non-patrimonial loss there is an impairment or disturbance of interests of personality which causes

412(...continued)
Aquilian action brought to establish a right, although no actual loss is proved, is contrary to principle, enjoys little modern support, and cannot be accepted" (Boberg *Delict* 475).

413 Neethling, Potgieter & Visser *Delict* 3; Van der Walt & Midgley *Delict* 29 (par 31).

414 Neethling, Potgieter & Visser *Delict* 212.

415 Visser et al *Damages* 24; Neethling, Potgieter & Visser *Delict* 212. In terms of this definition, damage is a broad concept which consists of patrimonial as well as non-patrimonial loss (Visser et al *Damages* 29; Neethling, Potgieter & Visser *Delict* 213).

416 Remarks by McQuoid-Mason*Privacy* 253 seem to suggest that he considers the patrimonial loss that flows from the infringement of privacy to be pure economic loss. However, pure economic loss is defined as loss that does not result from damage to the plaintiff's property or impairment of the plaintiff's personality, or where it does flow from that, such damage or injury was not caused by the defendant (see Neethling, Potgieter & Visser *Delict* 296; Visser et al *Damages* 59; Neethling & Van Aswegen 1989 *THRHR* 607 and Aswegen *Sameloop* 172). Since privacy and identity are part of the personality of the plaintiff, the loss involved does not fit this definition. Granted, when McQuoid-Mason's work was published, pure economic loss was narrowly defined as pecuniary loss suffered by a plaintiff where such loss does not flow from physical damage to the person or property of the plaintiff (see eg Boberg *Delict* 103; Van der Walt & Midgley *Delict* 77 (par 64)).

417 *Matthews v Young* 1922 AD 492; Boberg *Delict* 18.

a reduction in their quality or utility.[418] Non-patrimonial loss has objective as well as subjective elements or facets.[419] The objective element refers to the external manifestation of the impairment, whereas the subjective element exists in a person's mind or consciousness and is formed *inter alia* by his or her reaction to the objective impairment of the personality interest.[420] In some instances, such as privacy and identity, the objective element is the most important. The plaintiff's emotional reaction is of secondary importance; the core issue is to establish objectively that an infringement of privacy or identity has taken place.[421] Prospective non-patrimonial loss may also be claimed.[422]

The existence and quantum of non-patrimonial loss[423] are established by a comparative method.[424] The utility and quality of the personality interest in question (privacy or identity) before and after the event are compared in order to establish the existence and the extent of the loss. In this way information is obtained about the nature, seriousness, extent, intensity and duration of the objective part of the loss (the recognisable manifestation of the infringement of the personality right, for example the fact that the data controller has supplied incorrect or sensitive personal information on the data subject to hundreds of third parties) as well as the subjective part of the loss (plaintiff's emotional reaction, which is of secondary importance in cases of infringement of privacy and identity).[425]

418 Neethling, Potgieter & Visser *Delict* 242.

419 See Visser et al *Damages* 96.

420 Neethling, Potgieter & Visser *Delict* 242–243; Van der Walt & Midgley *Delict* 34 (par 35); Visser et al *Damages* 97.

421 Neethling, Potgieter & Visser *Delict* 243; Van der Walt & Midgley *Delict* 34 (par 35). Thus, a person's privacy and identity can be infringed even if he or she is not aware of this.

422 Neethling, Potgieter & Visser *Delict* 243.

423 Non-patrimonial loss is defined as "the diminution, as a result of a damage-causing event, in the quality of the highly personal (personality) interest of a person satisfying his legally recognised needs but which does not affect his patrimony" (Neethling, Potgieter & Visser *Delict* 242; Visser et al *Damages* 19).

424 Neethling, Potgieter & Visser *Delict* 242; Visser et al *Damages* 107.

425 Neethling, Potgieter & Visser *Delict* 242–243.

The existence and quantum of patrimonial loss[426] are also established by a comparative method.[427] The current patrimonial position of the plaintiff after perpetration of the delict is compared with the hypothetical patrimonial position[428] the plaintiff would have been in had the delict not been committed. The difference between the two positions constitutes the plaintiff's patrimonial loss.[429]

Mitigation of loss

The principle of mitigation of loss is relevant for both patrimonial and non-patrimonial loss. This principle entails that a plaintiff may not recover damages for a loss which could have been prevented if the plaintiff had taken reasonable steps to do so.[430] In other words, if a plaintiff suffers damage due to data processing, he or she should take reasonable steps to reduce the loss or to avert further loss. For example, as soon as a person realises that inaccurate data are being processed in relation to him or her, resulting in the plaintiff's identity being infringed and plaintiff suffering patrimonial loss (for example, the plaintiff is denied a financial benefit such as credit, or insurance coverage), he or she should take

426 Patrimonial loss is defined as "the diminution in the utility of a patrimonial interest in satisfying the legally recognised needs of the person entitled to such interest" (Neethling, Potgieter & Visser *Delict* 219; Visser et al *Damages* 45).

427 Van Aswegen *Sameloop* 160; Knobel *Trade secret* 253; Visser et al *Damages* 64.

428 A hypothetical patrimonial position is used to provide for instances where prospective damage, liability for misrepresentation and loss of profit is claimed (Neethling, Potgieter & Visser *Delict* 223). Prospective damage (*lucrum cessans*) is damage that will only materialise after the date of assessment of damage (Neethling, Potgieter & Visser *Delict* 224). However, the plaintiff must also claim for prospective damage when he or she claims for damage already sustained (*damnum emergens*), because of the "once and for all" rule which holds sway in our law. In terms of this rule the plaintiff must in an action for damages, claim for all damage already sustained or expected in future in so far as the claim is based on a single cause of action (Neethling, Potgieter & Visser *Delict* 226; Van der Walt & Midgley *Delict* 193 (par 135)).

429 Neethling, Potgieter & Visser *Delict* 222–223; Van Aswegen *Sameloop* 162. However, some authors argue that the correct method of comparison is to compare the difference between the patrimonial position of the prejudiced person before and after the wrongful act (Van der Walt *Sommeskadeleer* 284; Van der Merwe & Olivier *Onregmatige daad* 180). This so-called concrete comparative method has also been used by the Appellate Division (*Santam Versekeringsmaatskappy Bpk v Byleveldt* 1973 2 SA 146 (A) 150). Neethling, Potgieter & Visser *Delict* 223 suggest that the concrete concept of damage should be adopted in practice, but not in instances where prospective loss, liability for misrepresentation and loss of profit are claimed for, because a test with a hypothetical element is necessary for such instances. See also Visser et al *Damages* 67.

430 Neethling, Potgieter & Visser *Delict* 235; Van der Walt & Midgley *Delict* 205; Van der Merwe & Olivier *Onregmatige daad* 187. See eg *De Pinto v Rensea Investments (Pty) Ltd* 1977 4 SA 529 (A).

reasonable steps to inform the data controller that such data are inaccurate in order to prevent further processing of these data resulting in further patrimonial and non-patrimonial loss.

2.4 Delictual remedies

2.4.1 Introduction

The delictual remedies have either a preventive or a compensatory function.[431] The interdict, which is available to restrain a person from committing or continuing to commit a wrongful action, has a preventive function.[432] The *actio legis Aquiliae* compensates a plaintiff for patrimonial loss (*damnum iniuria datum*) sustained, and the *actio iniuriarum* is directed at providing satisfaction (*solatium*) for non-patrimonial loss in the form of injury to personality (*iniuria*). The action for pain and suffering is also aimed at compensation, namely for injury to bodily or physical-mental integrity.[433]

The applicability of the delictual remedies in the area of data protection can be illustrated with an example. Suppose that Y does business as a credit reference company. It incorrectly records that X is insolvent and reports this to Z, who uses Y to check the credit rating of potential customers. Z refuses to do business with X. As a result of this, X suffers an *iniuria*, because a personality interest of his, namely his right to identity, has been infringed.[434] If X can prove all the elements of the *actio iniuriarum*, X can sue Y for satisfaction. However, owing to the fact that Y refused to do business with X, X could also have suffered patrimonial loss and in order to recover that loss, X has to prove the requirements of the *actio legis Aquiliae*. In addition, X can obtain an interdict against Y, not only to

431 See Van Aswegen *Sameloop* 105.

432 Neethling, Potgieter & Visser *Delict* 260.

433 This action would only be relevant to data processing in exceptional cases, eg, if the infringement of the data subject's personality is of such a nature that it eventually causes emotional trauma to the data subject. Since it is not of great importance or relevance, this action will not be discussed any further.

434 See par 2.3.2.1 above.

correct the information, but also to prevent Y from further disclosure of the incorrect data.[435]

2.4.2 Actio iniuriarum

The requirements for the *actio iniuriarum* are, in general, well established. The plaintiff has to allege and prove[436] the wrongful and intentional infringement of his or her personality (in the above scenario, by the incorrect processing of plaintiff's personal data).[437] Intent (*animus iniuriandi*) is therefore required. This means that the defendant must have directed his or her will to violating the privacy or identity of the plaintiff, knowing that such violation would (possibly) be wrongful.[438]

Under the *actio iniuriarum*, once wrongful conduct has been established, there is a presumption of *animus iniuriandi* which the defendant may rebut.[439] Examples of defences that exclude intent are mistake and jest.[440] Jest as a defence is not relevant in the context of data protection. In the case of mistake, the element of consciousness of wrongfulness is absent. This would for example be the case where defendants do not realise that their processing of data is wrongful, because they are under the mistaken (but honest) impression that they have a valid ground justifying the processing.[441]

---

435 These remedies are a reflection of the data protection principle of accountability (see ch 6 par 2.2.10).

436 Elements not in dispute in a particular lawsuit need not be proved by the plaintiff (Knobel *Trade secret* 236).

437 Joubert *Grondslae* 77; *Jackson v NICRO* 1976 3 SA 1 (A) 1.

438 See par 2.3.3.2 above. Also see Neethling *Persoonlikheidsreg* 203; McQuoid-Mason *Privacy* 101. But see *C v Minister of Correctional Services* 1996 4 SA 292 (T) 304–305 where consciousness of wrongfulness was not required for liability of the government for the infringement of the privacy of a prisoner (for a discussion of this case, see Knobel 1997 *THRHR* 533).

439 *Jansen van Vuuren v Kruger* 1993 4 SA 842 (A) 849; Neethling *Persoonlikheidsreg* 71; Neethling, Potgieter & Visser *Delict* 356; McQuoid-Mason *Privacy* 104; Van der Walt & Midgley *Delict* 132 (par 100); Van der Merwe & Olivier *Onregmatige daad* 432.

440 Neethling *Persoonlikheidsreg* 202–203; Neethling, Potgieter & Visser *Delict* 349; McQuoid-Mason *Privacy* 236; Van der Walt & Midgley *Delict* 130 (par 99); Van der Merwe & Olivier *Onregmatige daad* 433–436.

441 *Maisel v Van Naeren* 1960 4 SA 836 (C); *Nydoo v Vengtas* 1965 1 SA 1 (A); Neethling, Potgieter & Visser *Delict* 349; Neethling *Persoonlikheidsreg* 201; McQuoid-Mason *Privacy* 236; Van der Walt & Midgley *Delict* 130 (par 99); Van der Merwe & Olivier *Onregmatige daad* 434.

2.4.2.1 Negligence liability

There are a number of South African authors who argue that in a developed community it does not make sense to persist with the intention requirement of the classical *actio iniuriarum* and that personality protection should be extended to include the negligent infringement of personality interests.[442] Arguments in favour of this notion are *inter alia* that the penal function of the *actio iniuriarum*[443] is outdated in the light of the distinction between criminal law and the law of delict – as a consequence there need not be such a marked distinction between the *actio iniuriarum* and the *actio legis Aquiliae* with regard to the fault element any more: both have a compensatory function.[444] Furthermore, the idea of delictual liability for negligent infringement of the personality has long been accepted in certain foreign legal systems.[445] Another important reason is the fact that since *National Media Ltd v Bogoshi*[446] the liability of the media[447] for defamation is no longer based on intent but on negligence,[448] showing that the classical *actio iniuriarum* does not afford satisfactory protection under

442 Neethling *Persoonlikheidsreg* 72; Knobel 2002 *THRHR* 24, 25; Van der Merwe & Olivier *Onregmatige daad* 246, esp fn 8; Pauw *Persoonlikheidskrenking en skuld* 212–215; Visser 1982 *THRHR* 168–174. Also see *Marais v Groenewald* 2001 1 SA 634 (T) 646; Neethling 2002 *THRHR* 24 *et seq*; 2002 *THRHR* 574, 583 fn 67.

443 In Roman and Roman-Dutch law the *actio iniuriarum* was a penal action, the primary purpose of which was to punish the wrongdoer - see Van der Walt & Midgley *Delict* 3 (par 2) fn 11.

444 See Van der Walt & Midgley *Delict* 183 (par 126) and Van der Merwe & Olivier *Onregmatige daad* 246. Van der Walt and Midgley argue that punishment is the function of criminal law and that the law of delict should focus on compensation. For further arguments, relating to *inter alia* the absence of procedural safeguards and double-jeopardy, see Van der Walt & Midgley *Delict* 183–184 (par 126). But see Visser et al *Damages* 178–179.

445 Pauw *Persoonlikheidskrenking en skuld* 215.

446 1998 4 SA 1196 (SCA). Also see *Marais v Groenewald* 2001 1 SA 634 (T) 644–646.

447 In *Marais v Groenewald* 2001 1 SA 634 (T) this principle was extended to certain non-media parties.

448 Under influence of English law our courts held for a long time that *animus iniuriandi* was not required for liability of the press for defamation and the press was held liable without fault (see eg *SAUK v O'Malley* 1977 3 SA 394 (A) 404–405 407; *Pakendorf v De Flamingh* 1982 3 SA 146 (A) 156–158). After the adoption of the 1993 and 1996 Constitutions in which the importance of the free flow of information and the role of the media were recognised, it became necessary to review this situation. (For a discussion of the position after the 1996 Constitution was adopted but before the *Boghoshi* case was decided, see Neethling *Persoonlikheidsreg* 73–74. Also see Neethling, Potgieter & Visser *Delict* 348, esp fn 205.) In *National Media Ltd v Bogoshi* 1998 4 SA 1196 (SCA) 1210–1211 the Supreme Court of Appeal made a turn-about, deciding that the *Pakendorf* case had been wrongly decided because it was in conflict with the democratic

(continued...)

all circumstances.

Neethling[449] expresses the hope that in future when other personality interests, such as privacy and identity, are weighed against interests such as freedom of speech, the influence of the Constitution will eventually lead to the acceptance of liability based on negligence.[450] Burchell[451] also argues for a negligence criterion on the Internet regarding the potential liability of a service or access provider for defamation, impairment of dignity or invasion of privacy. If negligence is accepted in future by the courts as the applicable fault criterion for the *actio iniuriarum* (and it is submitted that it should be accepted as a first step[452]), it would mean that the negligent processing of data will be a sufficient ground for a claim for non-patrimonial loss. In the area of data processing negligence liability will also bring about a fairer balance between the right to privacy and other rights such as freedom of information and freedom of data controllers to choose their trade, occupation and profession.[453]

448(...continued)
imperative that the public interest was best served by the free flow of information and the role of the media in the process. However, the court was not prepared to merely re-instate the common law position of liability based on *animus iniuriandi*, because it would then have been too easy for the media to rely on absence of consciousness of wrongfulness as a defence (Neethling, Potgieter & Visser *Delict* 348). Instead the court recognised negligence as a ground of liability for the media in defamation cases (see *National Media Ltd v Bogoshi* 1998 4 SA 1196 (SCA) 1214). See further Neethling, Potgieter & Visser *Delict* 348; Neethling and Potgieter 1999 *THRHR* 442. This view is supported by most authors (see eg Neethling & Potgieter 1994 *THRHR* 513, 517–518; 1995 *THRHR* 709, 713; 1996 *THRHR* 706, 710; Van der Walt 1998 *TSAR* 198, 209; Burchell *Delict* 184; *Personality rights* 320–322; Van Aswegen 1995 *SAJHR* 50–69; Knobel 2002 *THRHR* 24, 27; but see Midgley 1996 *THRHR* 635, 637–638 who prefers an "attenuated form of intention" – ie intention without consciousness of wrongfulness, and therefore only "the intention to achieve a particular result", ie direction of will), because it achieves a more equitable balance between the right to a good name and the right to freedom of expression and it is also in accordance with the values underpinning the Bill of Rights (Neethling, Potgieter & Visser *Delict* 348).

449 Neethling *Persoonlikheidsreg* 74.

450 In time, Neethling *Persoonlikheidsreg* 74 argues, this may lead to the development that the state and its organs will be liable for all personality infringements committed by its servants or organs, wrongly and negligently (or eventually even without fault). These developments may be justified by the obvious and general principle that human rights are intended to strengthen the legal position of subjects *vis-a-vis* the state and its organs.

451 Burchell *Personality rights* 124.

452 Eventually fault should cease to be a requirement (see below and see also Neethling 2002 *THRHR* 574, 583–584).

453 See par 2.3.2.3.c.i. above.

2.4.2.2 Strict liability

In South African law, fault is generally required for delictual liability.[454] Strict liability (liability without fault) occurs as an exception to the general rule in limited instances only. Examples of strict liability in South African law are certain instances of *iniuria*,[455] certain common law actions,[456] vicarious liability[457] and instances of statutory liability.[458]

The fault theory, namely that a wrongdoer should be held liable in delict only if he or she had fault, was the dominant theory in the 19th century.[459] The traditional basis of delictual liability was re-evaluated, however, during the latter part of the 19th century and the 20th century as a result of economic and technological developments which brought radical social and economic changes in their wake. Neethling, Potgieter and Visser explain:[460]

> Increased mechanisation and expanding technology in almost every facet of life, together with a corresponding and unprecedented exposure of individuals to the risk

454 Boberg *Delict* 16; Neethling, Potgieter & Visser *Delict* 119; Van Aswegen *Sameloop* 148.

455 Viz, wrongful deprivation of liberty and wrongful attachment of property (Neethling, Potgieter & Visser *Delict* 372). According to Van der Walt & Midgley *Delict* 2 (par 2) fn 12 and 128 (par 97) "intent takes an attenuated form" in these cases. But see Van der Merwe & Olivier *Onregmatige daad* 552–553.

456 Viz, the *actiones de pauperie, de pastu* and *de feris* (for damage caused by animals), the *actiones de effusis vel deiectis* and *positi vel suspensi* (for damage caused by objects thrown, poured or falling out of or from a building) and the *actio aquae pluviae arcendae* and *interdictum quod vi aut clam* and action for the disturbance of the lateral support (for damage caused by owners of neighbouring properties (see Neethling, Potgieter & Visser *Delict* 363–372; Van Aswegen *Sameloop* 115 fn 49 and 148; Van der Merwe & Olivier *Onregmatige daad* 486–508; Van der Walt & Midgley *Delict* 26–27 (par 25–28)). Van der Walt & Midgley *Delict* 27-28 (par 29) also mention the *condictio furtiva*.

457 In the case of vicarious liability one person is held strictly liable for damage caused by another. This liability applies in certain instances where there is a special relationship between two persons, eg employer-employee, principal-agent and motor car owner-motor car driver. See further Neethling, Potgieter & Visser *Delict* 373 *et seq*; Van der Merwe & Olivier *Onregmatige daad* 508 *et seq*; Van der Walt & Midgley *Delict* 24 (par 24).

458 Eg, the Legal Succession to the South-African Transport Services Act 9 of 1989; the Aviation Act 74 of 1962; the National Nuclear Regulator Act 47 of 1999 and the Post Office Act 44 of 1958 (see further Neethling, Potgieter & Visser *Delict* 381–383).

459 See further Neethling, Potgieter & Visser *Delict* 363.

460 Neethling, Potgieter & Visser *Delict* 363. See also Van der Walt *Risiko-aanspreeklikheid*; 1968 *CILSA* 49.

> of harm, drew attention to the inadequacy of the fault theory. Electricity, nuclear power, motor vehicles, aeroplanes and the like have created potentially dangerous situations for the individual in which he is virtually defenceless. [In the 21st century the risk created by the computer and modern information technology can surely be added to this list.[461]] The growing need to protect the individual caused the development, in Continental and Anglo-American legal systems, of a field of liability without fault (risk, absolute or strict liability). Likewise in South African law, certain instances of strict liability were imposed by legislation, while a growing number of judges and other jurists began to stress the need for the development of a field of delictual liability without fault over and above the traditional area of liability based on fault.

The increased liability which strict or faultless liability entails for the defendant is justified by factors such as:[462]

- the fact that the defendant created a high risk of damage
- the advantages which the creator of the risk draws from his or her products
- the greater degree of care that will result from an increased liability
- the possibility of transferring the risk by way of insurance to an insurer
- the fact that the wrongdoer exercises control over his or her enterprise and thus also over the risk he or she creates
- considerations of fairness in general

The risk or danger theory, which holds that where a person's activities create considerable increase in the potential for harm there is sufficient justification for holding him or her liable for damage even in the absence of fault,[463] seems to explain most of the instances of strict liability recognised in our law,[464] and

461 See ch 1 par 1.2; Alheit *Expert systems* 1; Neethling 2002 *THRHR* 574, 582–584.

462 Neethling, Potgieter & Visser *Delict* 364. See also Van der Walt *Risiko-aanspreeklikheid* 192 *et seq*.

463 Whether or not the potential of risk has been sufficiently increased, will depend largely on the legal (continued...)

in other legal systems.[465] Neethling[466] suggests that *de lege ferenda*, a person should be held liable without fault if he or she unlawfully[467] causes harm to another due to an extremely dangerous or risky activity. An activity would be extremely dangerous or risky if it creates a high risk of harm, if the extent of the possible harm would be serious, and if it is impossible to prevent harm even where reasonable care is taken.[468]

Faul[469] examines the theoretical possibility of holding a bank strictly liable for disclosing confidential information furnished to it by a client. She identifies the following factors as relevant in establishing a risk-based liability for the bank:

- A client who wants to make use of the services of a bank is obliged to furnish information to the bank.
- The client does not have any control over the further use or disclosure of the information.
- The risk is created that the client will suffer injury if the information is disclosed.
- Such injury can be very serious in the light of the speed with which information can be dispersed worldwide.
- The relationship between the client and the bank is not one of equality (*ongelykheids-verhouding*).
- The client would experience difficulty in proving fault on the part of the bank. The real actor is

463(...continued)
convictions of the community as reflected in legislation or case law (Van der Walt 1968 *CILSA* 49, 55).

464 Neethling, Potgieter & Visser *Delict* 364. In *Loriza Brahman v Dippenaar* 2002 2 SA 477 (SCA) Olivier JA said that "die verskynsel van risiko-aanspreeklikheid brei in die moderne tyd uit en vervul op gepaste terreine 'n nuttige funksie...". See further Neethling 2002 *THRHR* 574, 590.

465 Neethling 2002 *THRHR* 574, 590. Neethling points out that the principle is applicable in Germany, Austria, Belgium, England, France, and the USA.

466 Neethling 2002 *THRHR* 574, 591.

467 Grounds of justification that exclude wrongfulness should still be available for the defendant.

468 See authority cited by Neethling 2002 *THRHR* 574, 591 fns 107, 108.

469 Faul *Bankgeheim* 533 – 534. Her explanation refers to the idea of *normatiewe risiko skepping* of Van der Walt as explained in Van der Walt *Risiko-aanspreeklikheid*. See also Neethling 2002 *THRHR* 574, 590.

difficult to identify and disappears in the faceless banking enterprise. Since the client cannot identify the real actor, whose fault would he or she have to prove?

- The human hand of the actor disappears in the mechanisation of banking services.

These factors are, however, not only applicable to banks (as data controllers) and their clients (as data subjects). Many or all of these factors are also relevant in other relationships between data controllers and data subjects. However, in the bank-client relationship data subjects have knowledge of the fact that the bank processes information on them from time to time. In many other instances data subjects do not even know that their personal information is being processed by a particular data controller and they often do not have the opportunity to deal directly with the data controller. The risk of injury in these instances is therefore even more acute.

Neethling[470] is also in favour of recognising strict liability in actions for either satisfaction for non-patrimonial loss or compensation for patrimonial loss, where wrongful data processing caused the data subject harm.[471] He advances the following reasons for the strict liability for data controllers:

- The collection and use of personal data (especially by means of electronic data banks) poses a serious threat to an individual's personality.

- It is difficult to prove fault on the part of the controller.

- The individual's right to privacy, which is protected as a fundamental right in the Bill of Rights, deserves the greatest measure of protection against unlawful data processing.

---

470 Neethling *Persoonlikheidsreg* 333–334; Neethling 2002 *THRHR* 574, 583–584. See also Du Plessis *Reg op inligting* 393–394.

471 Burchell *Personality rights* 124 favours a negligence standard as far as the liability of Internet service providers for defamation, impairment of dignity or invasion of privacy is concerned, since he feels that strict liability of the publisher on the Internet would paralyse the transfer of information. However, since all the other elements of a delict, including wrongfulness, still need to be present (see below), this fear seems to be exaggerated.

- Strict liability serves as an encouragement for the data processing industry to act with as much care as possible.

- The data processing industry is, from an economic point of view, in the best position to absorb and distribute the burden of harm.[472]

The other elements of a delict, namely conduct, wrongfulness, causation and harm, should of course still be present. Liability for the plaintiff can therefore be excluded by the presence of a ground of justification, or of defences such as *vis maior* and fault on the part of the plaintiff.[473]

2.4.3 Actio legis Aquiliae

Where a plaintiff's privacy or identity is infringed because of wrongful data processing and such processing also caused patrimonial loss, the plaintiff can claim compensation for such patrimonial loss because "[o]ur law readily accepts that actions having different purposes can be based on the same set of facts. Thus a claim under the *actio iniuriarum* can exist together with one in contract, as well as with an *Aquilian action* and an action for pain and suffering".[474]

---

472 Neethling 2002 *THRHR* 574, 584. Neethling *Privaatheid* 363; 1980 *THRHR* 141, 152–153. This is the position under the EU Directive on data protection and the Netherlands WBP (see also ch 6 par 2.4). In terms of the EU Directive (which is applied almost verbatim in Dutch law), data subjects should be entitled to receive compensation from the controller for damage suffered as a result of an unlawful processing operation or of any act incompatible with such laws. Controllers may be exempted from this liability, in whole or in part, if they prove that they are not responsible for the event giving rise to the damage (Dir 95/46/EC a 23(2)). Examples of situations where the controller may be exempted are where the data subject was at fault, or in the case of *force majeure* (Dir 95/46/EC recitals par (55)). In the DP Act of the UK an individual who suffers damage by reason of any contravention by a data controller of any of the requirements of the Act is entitled to compensation from the data controller for that damage (DP Act of 1998 s 13(1)) but it is a defence for a data controller against such proceedings to prove that he or she had taken reasonable care to comply with the requirement in question (ie, that he or she did not act wrongfully as a result of impossibility as a ground of justification – see par 2.3.2.3.b.v above) (DP Act of 1998 s 13(3)). Under the USA Privacy Act actual damages can be claimed provided that the individuals can prove that the agency acted wilfully or intentionally and that the agency action affected them adversely (5 USC s 552a(g)(4)).

473 Neethling, Potgieter & Visser *Delict* 365. This is done in the EU Directive (see Dir 95/46/EC a 23(2) and recitals par (55)). Also see previous fn.

474 Van der Walt & Midgley *Delict* 44 (par 49).

To claim for patrimonial loss, the *actio legis Aquiliae* would be the appropriate action and in such a case negligence[475] is sufficient for liability.[476]

The defendant's liability should be limited if the plaintiff acted with contributory negligence. In such a case the damages recoverable by the plaintiff should be reduced to the degree in which the plaintiff was at fault in relation to the damage.[477]

It stands to reason that if strict liability for data processing is recognised as suggested above, negligence will no longer have to be proved.

2.4.4 Interdict

Data subjects who want to prevent an impending wrongful data processing, or to prevent the continuation of a wrongful data processing, may also apply for an interdict. The interdict may take the form of a prohibitory or mandatory court order. A prohibitory order prohibits the committing or continuing of a wrongful act (such as continuing to process incorrect data), whereas a mandatory order requires a positive action on the part of the wrongdoer to terminate the continuing wrongfulness of an act that has already been committed (such as correcting or deleting incorrect data).[478]

An interdict may be final or temporary (interim or interlocutory).[479] Our courts formulate the

475 See par 2.3.3.2 above on negligence.

476 Neethling, Potgieter & Visser *Delict* 262 328; McQuoid-Mason *Privacy* 253; Van Aswegen *Sameloop* 108. Also see *Mathews v Young* 1922 AD 492; *Minister of Finance v EBN Trading (Pty) Ltd* 1977 4 SA 376 (T) 385.

477 Apportionment of Damages Act 34 of 1956 s 1.

478 Neethling, Potgieter & Visser *Delict* 260–261; Van der Walt & Midgley *Delict* 178 (par 124); Van der Merwe & Olivier *Onregmatige daad* 250.

479 Neethling, Potgieter & Visser *Delict* 261; Van der Walt & Midgley *Delict* 179 (par 124); Knobel *Trade secret* 264.

requirements for a final interdict as follows:[480]

- a clear right[481]
- an actual or threatened invasion of the right
- the absence of another suitable remedy

The same requirements must be met for a temporary interdict, but a further requirement, namely that the balance of convenience must favour the granting of the interim interdict, must also be met.[482] The grant or refusal of an interlocutory interdict is always within the discretion of the court.[483] According to Van der Walt and Midgley, an interdict will, in general, be refused if the harm is small, if it is capable of being estimated in money and adequately compensated by the award of a small monetary payment, and if the granting of the interdict would be oppressive to the respondent.[484]

For the purposes of a delictual remedy in the case of data processing, these requirements can be formulated as follows: the existence of wrongful conduct (data processing which infringes the rights to privacy and identity) which either causes, or threatens to cause harm (infringement of privacy or identity) to the plaintiff.[485] Since the interdict has a preventive function, neither fault on the part of the wrongdoer nor damage are requirements for the remedy.[486]

The interdict can be a very useful remedy for a data subject who wants to put a stop to wrongful data processing, or to prevent such processing from taking place at all. Since fault is not a requirement even data processors who do not have the necessary intent to found the *actio iniuriarum* can be interdicted.

---

480 See eg *Setlogelo v Setlogelo* 1914 AD 221 227; *Patz v Greene and Co* 1907 TS 427; *Hall v Heyns* 1991 1 SA 381 (C) 395.

481 In other words, the right must be clearly established (see Knobel *Trade secret* 264).

482 *Knox D'Arcy Ltd v Jamieson* 1995 2 SA 579 (W) 593; Van der Walt & Midgley *Delict* 179 (par 124).

483 *Knox D'Arcy Ltd v Jamieson* 1995 2 SA 579 (W) 592; Van der Walt & Midgley *Delict* 179 (par 124).

484 Van der Walt & Midgley *Delict* 179 (par 124).

485 See Van der Walt & Midgley *Delict* 179 (par 124).

486 Neethling, Potgieter & Visser *Delict* 261. See also *Setlogelo v Setlogelo* 1914 AD 221 227.

A data subject also does not have to wait for damage to materialise before he or she can take action.

2.5 Problematic types of data subjects

2.5.1 Deceased persons as data subjects

From the comparative analysis, it is evident that there is a difference of opinion as to whether deceased persons can be data subjects. The debate usually centres around the interpretation of the term "individual", since data subjects are usually described as "identifiable individuals". One argument is that genetic profiling may justify protecting information on deceased persons, because the use of data concerning a deceased person can have repercussions for living relatives.[487]

However, it is evident that in our law a deceased person cannot be a data subject. The rights to privacy and identity which are the primarily protected interests involved in data protection are personality rights. Personality rights come into existence with the birth of a human being and are terminated by his or her death.[488] Our law also does not recognise *iniuria per consequentias* in the sense that an *iniuria* against one person automatically also constitutes an *iniuria* against someone else in a special relationship with that person.[489] It is required that the *iniuria* must have been committed against the plaintiff himself or herself.[490] The processing of information on a deceased person will therefore only constitute an *iniuria* towards a living individual if he or she can prove that the processing intentionally infringes his or her personality. It may, for example, constitute an unlawful infringement of the feelings of a living relative of the deceased if sensitive information about the him or her is processed.[491]

487 Pounder & Kosten 1995 (21) *Data Protection News* 6; Laurie *Genetic privacy* 3, 116–117.

488 Neethling *Persoonlikheidsreg* 17.

489 See *Meyer v Van Niekerk* 1976 1 SA 252 (T) 256; *Spendiff v East London Daily Dispatch Ltd* 1929 EDL 113, 129–130; Neethling *Persoonlikheidsreg* 77; McKerron *Delict* 55.

490 *Spendiff v East London Daily Dispatch Ltd* 1929 EDL 113, 129–130; *Goodall v Hoogendoorn Ltd* 1926 AD 11, 15; *SA Associated Newspapers Ltd v Schoeman* 1962 2 SA 613 (A); *Miller v Abrahams* 1918 CPD 50.

491 Neethling *Persoonlikheidsreg* 245 fn 19; Van Wyk 1996 *THRHR* 626, 632–633. The definition of personal

(continued...)

Where information on a deceased person also relates to living individuals, the living individuals will be protected in their own right.

2.5.2 Juristic persons as data subjects

2.5.2.1 Introduction

Whether juristic persons could be considered to be data subjects depends on whether they possess a right to privacy and a right to identity.[492] Westin[493] defines the right to privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others". From this definition, which according to Nugter has been widely accepted in European law,[494] it would seem that juristic persons also have a right to privacy. However, most international documents, such as the OECD Guidelines, the Council of Europe Convention and the European Union Directive, apply to individuals only. Parties to the Convention may extend the scope of their legislation to include groups of persons, with or without legal personality, as

491(...continued)
information in the Promotion of Access to Information Act 2 of 2000 includes information on individuals who have been dead for less than twenty years. The Act also provides that access to information kept by a private or public body must be refused where the disclosure of the information would involve the unreasonable disclosure of personal information about a third party, including a deceased person (s 34 and s 63). Access may not be refused to information about a deceased person if the person making the request is the individual's next of kin, or is making the request with the written consent of the next of kin (s 34(2) and 63(2)). It is submitted that the Act is not protecting the right to privacy of the deceased person, but is protecting the rights of the next of kin (such as their right to feelings of piety) or (an unspecified) public interest.

492 A government may of course also consider policy issues when deciding whether juristic persons should be granted the status of "data subjects" in a data protection act. International trends should *inter alia* play an important role. As indicated, legislators should strive to harmonise data protection laws, since this enhances the free flow of information and avoids conflict of laws problems (see Sieghart "Protection of personal data" 224–229; also see ch 3 par 1 and ch 6 par 1.2). See also Bygrave *Data protection laws* 178 who emphasises that whether or not the basic data protection principles should be extended to collective entities can only be determined for a particular country on the basis of a consideration of the need for extending such protection.

493 Westin *Privacy and freedom* 7.

494 See Nugter *Transborder flow of personal data* 16.

data subjects.[495] However, none of the countries researched in this thesis has extended protection to juristic persons.[496]

According to Bygrave there was a lot of support for giving "collective entities"[497] data protection rights in the early stages of data protection legislation – in fact the first data protection law in the German Land Hesse made no distinction between natural and legal (juristic) persons.[498] Five countries, Norway, Denmark, Austria, Luxembourg and Iceland enacted national data protection laws towards the end of the 1970s and early 1980s expressly covering data on both juristic and natural persons. However, this trend did not continue. The majority of data protection laws adopted since then applied to individuals only. The exception was Switzerland (in 1992) and Italy (in 1996).[499] When Iceland and Norway adopted new data protection laws in 2000, they both dispensed with the protection of collective entities. The new law in Denmark (also adopted in 2000) retained protection for enterprises only in so far as data on them are processed by credit reporting agencies. On the other hand, Austria's new Act of 2000 retained the full ambit of protection for collective entities.[500]

The following reasons are usually advanced for excluding collective entities from data protection instruments:[501]

---

495 See ch 6 par 1.3.2.1. See also Burkert 1986 *Computer L & Prac* 155, 157; Turn *Transborder data flows* 81.

496 See ch 2 par 4.2.2.3 and par 4.3.2.2; ch 3 par 2.2.4 and par 4.2.3; ch 4 par 4.3.3 and ch 5 par 4.3.3.

497 Bygrave *Data protection law* 1 defines "private collective entities" as organised groups in the private sector. An organised group is one whose members take specific, systematic measures to establish and maintain it, eg business corporations and citizen initiative groups. Organised groups include those groups that are juristic persons and those that are not (Bygrave *Data protection law* 173). Organised groups can be distinguished from non-organised groups, which are groups of persons sharing one or more characteristics, eg ethnic origin, sexuality or religious beliefs. Bygrave also distinguishes between collective entities and one-person enterprises which are not collective entities (Bygrave *Data protection law* 174).

498 Bygrave *Data protection law* 179.

499 Bygrave *Data protection law* 179.

500 Bygrave *Data protection law* 195.

501 See Bygrave *Data protection law* 196 *et seq* for more detail. Reasons that are advanced as to why juristic persons should be considered to be data subjects include the fact that in the case of small companies data

(continued...)

- The main values and interests served by data protection laws are only applicable to individuals.[502]

- Collective entities, particularly corporations, do not need data protection rights because the individuals who constitute them enjoy such rights already or because the data protection interests of the entities as such are sufficiently protected under other legislation.

- Governments are generally disinclined to introduce rules that might further curtail their agencies' ability to process information on any sort of entity.

- There is a fear that expanding the class of data subjects to embrace collective entities will also expand the potential of these laws to restrict transborder flows of data that are important for international business transactions.

- There is uncertainty[503] over the ways in which the extension of data protection rights to collective entities would affect corporate activities, marketplace competition and the operation of other branches of the law.[504]

501(...continued)
relating to the company may also concern its owner or owners and provide information of a more or less sensitive nature (see OECD Guidelines Explanatory Memorandum 24; Gassmann "Privacy implications of transborder data flows" 109) and the (rather general) statement that fair information practices should also apply when decisions are made about juristic persons (see Turn *Transborder data flows* 813).

502 According to Bygrave *Data protection law* 196 this factor appears to have played a major role in the decisions of Sweden and the USA not to extend their respective data protection laws to juristic persons. It also explains the decision to drop express protection for juristic persons from the new Norwegian data protection legislation. Also see Girot & De Wit "Privacy van ondernemingen" 139, 149 *et seq*.

503 Bygrave *Data protection laws* 197 laments the "paucity of studies on the relationship between data protection and other fields of activity, and on the actual consequences of those laws that presently provide collective entities with data protection rights".

504 This uncertainty sometimes gives way to specific fears, eg that extending coverage of data protection laws to juristic persons would decrease corporations' transparency, thus hindering public control of their activities; or that corporations will use their data protection rights to distort economic competition between themselves (Bygrave *Data protection laws* 197).

❒ Major business groups are opposed to extending the ambit of data protection legislation to cover data on juristic persons.[505]

A motive for giving data protection rights to collective entities[506] is the belief on the part of the legislators involved that the social, political and economic implications of modern information technology are so pervasive that they threaten the interests of not just individuals but also collective entities.[507] It also appears that it was considered especially necessary to protect small businesses in the credit reporting context.[508]

Bygrave argues that the core principles of data protection laws are logically capable of being extended to protect data on collective entities (organised and non-organised). He is also of the opinion that collective entities are capable of sharing most of the interests of data subjects which data protection laws typically safeguard. In the end the decisive issue is whether the basic principles of these laws **should** be extended to protect collective entity data and this, he argues, can only be determined for a particular country on the basis of the **need** for extending such protection. This need depends on (a) the economic, political and social roles that the various entities actually play in the country concerned; (b) the economic, political and social roles that the country desires the various kinds of collective entities to play; (c) the extent to which granting collective entities data protection rights would promote the chance of these entities fulfilling these desired roles; (d) other aspects of the country's legal system and

505 During the debate in 1976 and 1977 on the initial proposal by French legislators to enact data protection legislation covering data on juristic as well as natural persons, there was pressure from business groups to exclude protection of data relating to any kind of juristic person. Opposition to the proposal came from IBM, insurance companies and the Bank of France. A few years earlier, (West) German proposals to enact national data protection legislation covering data on both juristic and natural persons had also met with opposition from business groups. Similarly, Luxembourg's Chamber of Commerce came out strongly against its country's enactment of data protection legislation covering data on juristic persons, and the International Chamber of Commerce considered such protection to be "inappropriate, unnecessary and harmful". See further Bygrave *Data protection laws* 197–198.

506 See Bygrave *Data protection laws* 186. Bygrave points out that little material exists setting out why Austria, Denmark, Iceland, Italy, Luxembourg, Norway and Switzerland have enacted data protection statutes expressly regulating the processing of data on juristic persons. Documents accompanying the statutes either give no reason, or the reasons are not well articulated .

507 Bygrave *Data protection laws* 187.

508 Bygrave *Data protection laws* 188.

culture, including the manner in which its various laws currently protect data on different sorts of collective entities.[509]

2.5.2.2 *South African position*

In South African law, as indicated, the remedy for an infringement of a personality right is the *actio iniuriarum*.[510] Traditionally it is accepted that the function of the *actio iniuriarum* is to provide *solatium* or solace money (satisfaction) for the infringement of the plaintiff's personality, in other words for the person's injured feelings or sentimental loss. Strictly speaking this means that the *actio iniuriarum* cannot be available for a juristic person because it has "no feelings to offend or outrage".[511] However, there are instances where personality infringement can exist without injured feelings, in other words, without the plaintiff actually suffering sentimental or affective loss.[512] Neethling[513] therefore argues that in those instances juristic persons can also have personality rights. These rights are the right to a good name, the right to privacy and the right to identity.[514] This viewpoint is also accepted by the Bill of Rights which provides that juristic persons are entitled to the rights in the Bill of Rights to the

509 See Bygrave *Data protection laws* 178.

510 See par 2.4.2 above.

511 *Caxton Ltd v Reeva Forman (Pty) Ltd* 1990 3 SA 547 (A) 561;*Die Spoorbond v SAR; Van Heerden v SAR* 1946 AD 999 1011; *Universiteit van Pretoria v Tommie Meyer Films (Edms) Bpk* 1979 1 SA 441 (A).

512 Neethling *Persoonlikheidsreg* 65 gives the following examples: Where an unconscious person is assaulted; or the physical freedom of someone who is asleep, is restricted; or a woman is secretly observed while undressing; or defamation or infringement of someone's identity takes place while the victim is unaware that it is happening.

513 Neethling "Privaatheid en universiteite" 125; *Persoonlikheidsreg* 89–91; Neethling 1993 *THRHR* 704, 705; Neethling & Potgieter 1991 *THRHR* 120, 124–125. See also Dendy 1990 *BML* 149–152. South African courts recognise that juristic persons have a right to a good name and a right to privacy (see par 2.5.2). This approach is also favoured by Burchell *Personality rights* 394 who argues that "the conferment of a right to privacy ... on juristic persons is in keeping with the imperative [of the Constitution] of equality and equal treatment". As to the right to identity of juristic persons, see Neethling *Persoonlikheidsreg* 91.

514 A juristic person does not have a body or feelings and as such does not have a subjective right to physical integrity, nor to dignity or to feelings (see Neethling *Persoonlikheidsreg* 89; Burchell *Personality rights* 393).

extent required by the nature of the rights and the nature of the juristic person involved.[515]

Neethling accepts as a point of departure that the right to privacy of a juristic person is analogous to that of a natural person.[516] He defines the right to privacy of a juristic person as corporate condition of seclusion from the public and publicity which includes all those facts regarding the juristic person which the juristic person itself determines to be excluded from the knowledge of outsiders and in respect of which it evidences a will for privacy.[517]

The courts adopted the same approach. *Financial Mail (Pty) Ltd v Sage Holdings Ltd*[518] and *Janit v Motor Industry Fund Administrators (Pty) Ltd* [519] both concerned the right to privacy of juristic

515 Act 108 of 1996 s 8(4). According to Devenish *SA Bill of Rights* 22–23, a discretion has been accorded to the courts to determine which rights are capable of being exercised by juristic persons. He points out that there are certain rights that by their very nature cannot vest in juristic persons (eg human dignity, life, and freedom and security of person), whereas others are "eminently appropriate rights that vest in juristic persons" (eg rights to property, freedom of expression, occupational freedom and access to the courts and free trial). Other rights "apply by definition to juristic persons" (eg rights of trade unions and employer's organisations). Devenish argues that the legal position of juristic persons as regards the rights to privacy and reputation might be more problematic.

516 Neethling "Privaatheid en universiteite" 125, 129; *Persoonlikheidsreg* 40.

517 "Dit [privacy of a juristic person] is 'n korporatiewe toestand van afsondering van openbaarheid, wat al daardie feite aangaande die regspersoon omvat wat hyself bestem het om van kennismaking deur buitestaanders uitgesluit te wees en ten opsigte waarvan hy 'n privaathoudingswil het" (see Neethling "Privaatheid en universiteite" 125, 130; *Persoonlikheidsreg* 40 fn 331).

518 1993 2 SA 451 (A). In that case Corbett CJ referred to cases dealing with a corporation's right to sue for defamation, (*G A Fichardt v The Friend Newspapers Ltd* 1916 AD 1; *Dhlomo NO v Natal Newspapers (Pty) Ltd* 1989 1 SA 945 (A); *Caxton Ltd v Reeva Forman (Pty) Ltd* 1990 3 SA 547 (A); *Argus Printing and Publishing Co Ltd v Inkatha Freedom Party* 1992 3 SA 579 (A)) to illustrate that "as a matter of general policy, the Courts have, in the sphere of personality rights, tended to equate the respective positions of natural and artificial (or legal) persons where it is possible and appropriate for this to be done" (at 461). Defamation is one area where it is possible to do this, because "(a)lthough a corporation has no feelings to outrage or offend, it has a reputation (or *fama*) in respect of the business or other activities in which it is engaged which can be damaged by defamatory statements..." (at 462). The court also referred with approval to the viewpoint of Neethling, Potgieter and Visser *Deliktereg* 2nd ed (1992) 324 that a juristic person can also have a right to privacy because in this instance injury to personality can also exist without an injury to feelings.

519 1995 4 SA 293 (A). In that case tape recordings of meetings of the board of directors of the respondents were stolen and given to the appellant. These tape recordings contained privileged information concerning litigation between the appellant and the respondents, as well as other confidential information concerning the respondents. In the court *a quo* the respondents obtained an interdict against the appellant, in order

(continued...)

persons. In those cases the Appellate Division recognised that a juristic person has a right to privacy in respect of confidential discussions of the board of directors' telephone (business) conversations or written documents that relate to the juristic person's internal affairs.

The right to privacy of a juristic person should be distinguished from other interests, for example confidential business information or trade secrets, in respect of which an independent immaterial property right exits.[520] The privacy rights of individuals associated with the juristic person, for example employees, officers, or directors, should also be carefully distinguished from that of the juristic person.[521]

The processing of true information on a juristic person which the juristic person considers to be private, will consequently infringe the juristic persons's privacy, provided that the information does not involve trade secrets or personal information of an individual associated with the juristic person.

The processing of false or untrue information about the juristic person, on the other hand, will infringe the juristic person's right to identity. A juristic person's identity is manifested through *indicia* which distinguish it from other juristic persons. The identity of a juristic person is usually created by distinctive marks which are the object of a substantive immaterial property right, but should not be confused with such immaterial property right. Whereas the immaterial property right is infringed by "passing off", the right to identity is infringed if the *indicia* of the juristic person are used in a manner that cannot be

519(...continued)
to prevent him from using the information on the tape recordings during the litigation between them. Eksteen JA dismissed appellants appeal against the order. He pointed out that the theft of the tape recordings was an unlawful invasion of the privacy of the board of directors for which there was no justification. Since the information on the tapes was obtained by means of an unlawful intrusion upon the privacy of the respondents, any subsequent disclosure of that information would itself constitute an invasion of respondent's privacy (303).

520 Whereas trade secrets of a juristic person always have economic value, privacy does not have economic value, being an aspect of a juristic person's personality (Neethling "Privaatheid en universiteite" 125, 130; *Persoonlikheidsreg* 40 fn 331). Also see Knobel *Trade secret* 218–221.

521 Neethling "Privaatheid en universiteite" 125, 130; *Persoonlikheidsreg* 40 fn 331.

reconciled with the true image of the juristic person.[522] An infringement of identity and a distinctive mark may occur at the same time and be caused by the same conduct. When non-defamatory untrue information concerning a juristic person is published, there is in addition to the possible infringement of the right to goodwill, also an infringement of the juristic person's identity.[523]

As said, juristic persons are also entitled to the rights in the Bill of Rights to the extent required by the nature of the rights and the nature of that juristic person.[524] Given the fact that the courts have held that juristic persons have private law right to privacy and, by implication, to identity, it is submitted that they are also entitled to constitutional protection of their rights to privacy and identity.[525]

In the *Hyundai Motor Distributors* case[526] the Constitutional Court held that juristic persons do enjoy the right to privacy, although not to the same extent as natural persons. According to the court[527] juristic persons' privacy rights can never be as "intense" as those of human beings. Currie and Klaaren[528] point out that "the reason for this has less to do with legitimate expectations of privacy than with the fact that the core of the right to privacy is grounded in human dignity. Since juristic persons are not the bearers of human dignity, their privacy is less deserving of protection".
But this does not mean that juristic persons' privacy should not be protected. The court was of the opinion that the exclusion of juristic persons would lead to the possibility of grave violations of privacy in our society.

522 See Neethling *Persoonlikheidsreg* 91.

523 See Neethling *Persoonlikheidsreg* 91.

524 Act 108 of 1996 s 8(4). See also fn 515.

525 On the personality rights of juristic persons, see par 2.5.2.

526 *Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd* 2001 1 SA 545 (CC) 557. Also see par 2.3.2.2

527 *Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd* 2001 1 SA 545 (CC) 557.

528 Currie & Klaaren *AIA commentary* 118 (par 8.3).

> The state might, for instance, have free licence to search and seize material from any non-profit organisation or corporate entity at will. This would obviously lead to grave disruptions and would undermine the very fabric of our democratic state. Juristic persons therefore do enjoy the right to privacy, although not to the same extent as natural persons. The level of justification for any particular limitation of the right will have to be judged in the light of the circumstances of each case. Relevant circumstances would include whether the subject of the limitation is a natural person or a juristic person as well as the nature and effect of the invasion of privacy.[529]

Privacy rights protecting "personal autonomy" in the sense of the right to make decisions on one's body, and on sexual and familial relationships[530] can of course only be accorded to human beings,[531] but it seems consistent with the nature of juristic persons that they should be able to claim "informational" privacy rights.[532]

2.5.2.3 *Conclusion*

Both natural and juristic persons should be protected by a South African data protection law. It is theoretically sound in the South African law context, which recognises that juristic persons have a right to privacy[533] and by implication also a right to identity,[534] to include them as data subjects under a data protection regime.

---

529 *Investigating Directorate: Serious Economic Offences v Hyundai Motor Distributors (Pty) Ltd* 2001 1 SA 545 (CC) 557.

530 See fn 117.

531 A juristic person may have privacy rights protecting personal autonomy, however, in the sense of having the right to make decisions about private company operations.

532 See further McQuoid-Mason "Constitutional privacy" 18–18. See also par 2.3.2.1 above.

533 See par 2.5.2.

534 See eg *GA Fichardt Ltd v The Friend Newspapers Ltd* 1916 AD 1.

3 SUMMARY

The individual interests that data protection aims to protect are privacy and identity. Private law, especially the law of delict, provides a solid basis for data protection. Some of the data protection principles, for example the principles of fair and lawful processing, purpose specification, minimality, quality, disclosure limitation, confidentiality and accountability are reflected in traditional delictual principles. Data subjects should include both individuals and juristic persons, but not deceased persons.

4 ACTIVE CONTROL PRINCIPLES

4.1 Introduction

As said, some of the data protection principles are reflected in or can be based on traditional principles of delict. However, data protection principles such as openness, data subject participation and security are not so reflected. Nevertheless, all of them are directly or indirectly related to providing the data subject (active) control over his or her data processing. Seen in this light they all concern the essence of the (right to) privacy, namely the power or ability of a person to determine the scope of his or her interest in privacy.[535] The so-called active control principles affirm this traditional power and can dogmatically thus be firmly based on it.

It is clear that traditional delictual principles[536] provide only limited protection for an individual's personal information, because it does not give the individual active control over personal information that is being processed. The traditional principles are useful in determining whether processing of personal information has taken place lawfully or not. In the case of unlawful infringement, the individual can approach the courts for a remedy.[537] However, the traditional principles cannot ensure, for

535 See par 2.3.2.1.a.i

536 See Neethling *Persoonlikheidsreg* 329.

537 See par 2.4 above.

example, that the data subject has knowledge of the fact that his or her personal information has been collected, or that he or she has access to the information, or that he or she may correct incorrect information. For this reason, the recognition of "active control principles"[538] is necessary. When a person has active control over his or her personal data, even the traditional principles of data protection will be enhanced and play a more meaningful role.[539]

4.2 Active control principles[540]

4.2.1 Knowledge of existence of data processing

The most comprehensive measures for protecting data are worthless if the individual does not have knowledge of the existence of data concerning him- or herself processed by a data controller.[541] Without this knowledge he or she remains completely unaware that his or her privacy is threatened or even actually infringed. Therefore the data controller should have a legal duty to notify persons concerning whom data are collected of this fact (unless, of course, they are in some other way already aware of it). Obviously allowance must be made for exceptions to this principle, for example where personal information is processed for the purposes of national security.[542] This active control measure is a reflection of the data protection principle of openness or transparency.[543]

538 Neethling *Persoonlikheidsreg* 334 *et seq*.

539 Where the data subject has active control over his or her personal data he or she can establish whether processing takes place lawfully, in other words whether all the data protection principles such as purpose specification, minimality, quality and disclosure limitation are complied with.

540 See in general Neethling *Persoonlikheidsreg* 363 *et seq*. Regarding the duty of banks to their clients in this regard, see Meiring *Betalingstelsel* 357–358; Faul *Bankgeheim* 527–528.

541 Neethling *Privaatheid* 363; 1980 *THRHR* 151–152; Du Plessis *Reg op inligting* 393–394; McQuoid-Mason *Privacy* 195 *et seq*; 1982 *CILSA* 135 140 155; Klopper *Kredietwaardigheid* 264–267.

542 See Neethling "Databeskerming" 125–128; see also ch 6 par 2.2.8.

543 See ch 6 par 2.2.7.

4.2.2 Knowledge of purpose of data processing

Since the purpose(s) of data processing must be lawful (that is, for the protection of a legitimate private interest or the public interest), and the purpose simultaneously also determines the limits of lawful processing,[544] it is necessary that the individual must have knowledge of this purpose. If he or she is unaware of it, he or she can hardly be expected to judge whether processing which is taking place is lawful. Therefore, unless they are already aware of it, the data controller must notify the individuals concerned of the purpose of the data processing.[545] Once more, this is a reflection of the data protection principle of openness or transparency.[546]

4.2.3 Right of access

Once the data subject has knowledge of both the fact that data processing on his or her personal information is taking place, and the purpose of such processing, the data controller must allow the individual concerned reasonable access to his or her data file if the individual should request this.[547] Access should be given in the form necessary to accommodate the physical form of the stored record. For example, if the record is a written or printed file, a copy thereof should be provided; if the record consists of visual images, the visual images should be reproduced; if the record consists of sound recordings, it should be arranged for the sound recording to be heard, or it should be transcribed. If the record is held on a computer or in electronic or machine-readable format, a printed copy should be given.[548] Access should be given in a form and language understandable to the data subject. This active

544 See par 2.3.2.3.c above.

545 Neethling "Databeskerming" 127; Du Plessis *Reg op inligting* 418.

546 See ch 6 par 2.2.7.

547 The fundamental right of access to information kept by the state, or by any other person where such information is required for the exercise or protection of any rights, (s 32(1)(a) and (b) of the Constitution, 1996) now protects the data subject's right of access to his or her personal data. This fundamental right was given detailed practical functioning and application by the promulgation of the Promotion of Access to Information Act 2 of 2000. See further ch 8 par 4.2

548 See also Act 2 of 2000 s 29(6) (ch 8 par 4.2.6.10).

control measure is a reflection of the data protection principle of data subject participation.[549]

This right of access is necessary for effective and equitable control of data processing, for only thus will such a person be able to ascertain whether the information is correct, necessary for the purposes of the statute in question, necessary for the protection of a legitimate interest, etcetera.[550] Of course, there may be exceptions to the right of access to data in particular circumstances.[551]

4.2.4 Knowledge of third party access

In addition to the right of access to his or her personal data, an individual must also have the right to require from the data controller information as to the identity of all persons who have had access to this data. This will enable him or her to ascertain whether or not the information was used for the specified purpose(s) of the data processing and therefore for the protection of a legally recognised interest. Thus the data controller must be legally obliged, at the request of the individual, to give him or her information concerning whom and when the data were made available.[552] Obviously provision must be made for exceptions in situations where it will not be justifiable to disclose such information.[553] This is also a reflection of the data protection principle of openness or transparency.[554]

549 See ch 6 par 2.2.6.

550 This power is recognised in all foreign statutes dealing with data protection (see ch 6 par 2.2.6). See also De Klerk 1991 *SALJ* 166–170 on the right of patients to have access to their medical data, and Neethling "Privaatheid en universiteite" 137 on the right of students to have access to their student files, as well as Meiring *Betalingstelsel* 357 and Faul *Bankgeheim* 528–529 on the right of clients of banks to have access to their records at the bank.

551 See fn 542 above. Also see ch 8 par 4.2.7.

552 Neethling Persoonlikheidsreg 335; see also ch 6 par 2.2.5.

553 See fn 542.

554 See ch 6 par 2.2.7.

4.2.5 Right to request correction or deletion of data

The individual must have the power to procure a correction of misleading data, or the deletion of data which are false or obsolete, or data obtained in an unlawful manner, or data not reasonably connected with or necessary for the specified purpose. This right is essential for preventing or terminating an infringement of the individual's personality interests and is a reflection of the data protection principle of data subject participation.[555]

4.3 Security measures

From the comparative research, it is evident that the data controller must be under an obligation to implement appropriate technical and organisational measures to protect the integrity of personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access and against all other unlawful forms of processing.[556] The measures must ensure a level of security that is appropriate to the risks presented. Factors that are relevant in determining the appropriateness of the measures are:

- the state of the technology
- the cost of implementation
- the nature of the data to be processed

Should the controller choose a processor to do the processing on its behalf, the controller remains responsible for security and is required to choose a processor that will provide sufficient guarantees in respect of the technical and organisational security measures, and must complete a written contract with the processor, stipulating that the processor will act only on instructions from the controller, and that the security provisions are also incumbent on the processor.[557]

555 See ch 6 par 2.2.6; Neethling *Persoonlikheidsreg* 335.

556 See ch 6 par 2.2.4.

557 See ch 3 par 4.2.4.9. Also see ch 4 par 4.3.4.8 and ch 5 par 4.3.4.1.f. This is a reflection of the security and (continued...)

Although the present data protection principle of security and confidentiality cannot be classified under the active control principles, it nevertheless assist the data subject to maintain the integrity of his or her data and in this way indirectly to control such integrity.

5 SUMMARY: GENERAL PRINCIPLES OF DATA PROTECTION

As has been said,[558] private law, especially the law of delict, provides a solid albeit not complete basis for data protection. Some of the data protection principles are reflected in traditional principles of delict, while others, especially the principles of openness, data subject participation, and security are not so reflected. These principles should therefore be introduced into our law.

The introduction of a data protection regime can only be attained through the legislator and not the courts, for two reasons: First of all, in view of the inherent conservatism of the courts, as well as the fact that the protection of privacy and identity is still in its infancy in South African law, it is improbable that the application of the traditional data protection principles by the courts will occur often or extensively enough in the near future.[559] Secondly, as was emphasised in *Carmichele v Minister of Safety and Security (Centre for Applied Legal Studies Intervening)*,[560] the most important force behind legal reform is the legislator and not the judiciary. Since the introduction of a new data (privacy) protection regime is not merely an incremental change of the law, but a sometimes radical departure from existing law and an extensive regulation of the present field, it is a task for the legislator.[561] As has been pointed out, the recognition of the right to privacy in the Bill of Rights compels the legislator to introduce such

557(...continued)
confidentiality principle (see ch 6 par 2.2.9).

558 See par 3.

559 See Neethling *Persoonlikheidsreg* 328.

560 2001 4 SA 938 (CC). See par 2.2.2.

561 Neethling 2002 *THRHR* 574, 587. Compare also the view of the Supreme Court of Appeal with regard to the introduction of strict manufacturer's liability (*Wagener and Cuttings v Pharmacare Ltd* 2003 4 SA 285 (SCA)).

legislation.[562]

It is submitted – as proposed by Neethling[563] and expanded in the light of the comparative conclusions – that the following general principles should form the basis of any data protection law:[564]

(a) Data may be processed only for a specified lawful purpose or purposes.[565]

(b) Data which are processed for a specified purpose –
  (i) must be reasonably connected with, and necessary for, that purpose;[566]
  (ii) may not be used or communicated in a manner incompatible with that purpose;[567] and
  (iii) may not be stored or used for longer than is reasonably necessary for that purpose.[568]

(c) Processed data must
  (i) be true;
  (ii) not be misleading;[569] and

562 See par 2.3.2.2.

563 See in general Neethling *Persoonlikheidsreg* 336–337; see also Neethling "Databeskerming" 125–126; "Privaatheid en universiteite" 133; 2002 *THRHR* 574, 583–584; 1992 (1) *Codicillus* 4, 6–7; Schulze 1994 *THRHR* 75, 80–86; Burchell *Personality rights* 398–399; Burns *Communications law* 202–203.

564 No specific provision is made for the principle that the data processing should be lawful and fair. This principle is self evident and is in any case reflected in the principles stated below.

565 This will make data processing lawful (see par 2.3.2.3 above). It reflects the data protection principle of fair and lawful processing, as well as the purpose specification principle (see ch 6 par 2.2.1 and 2.2.2).

566 This reflects the minimality principle of data protection (see ch 6 par 2.2.3).

567 This reflects the disclosure limitation principle of data protection (see ch 6 par 2.2.5).

568 This also reflects the minimality principle of data protection (see ch 6 par 2.2.3). The principles mentioned in paragraph (b) will all ensure that the processing does not exceed the bounds of the ground of justification present.

569 Untrue and misleading data infringe on a person's right to identity (see par 2.3.2.1.b. above). The fact that data must be true and not misleading reflects the data quality principle of data protection (see ch 6 par 2.2.4).

(iii) have been obtained in a lawful manner.[570]

(d) A data subject[571] shall be entitled to –

(i) be aware of the existence of processed data on himself or herself processed by the data controller;[572]

(ii) be aware of the purpose(s) for which such data are processed;[573]

(iii) be afforded reasonable access to data concerning him or her stored by the data controller;[574]

(iv) be informed by a data controller to which third parties the data were communicated by that controller;[575]

(v) procure or effect a correction of misleading data at the data controller; and

(vi) procure or effect a deletion of false data, or obsolete data, or data obtained in an unlawful manner, or data not reasonably connected with or necessary for the purpose specified at the data controller.[576]

(e) Special provisions should be made for the processing of sensitive data,[577] as well as the processing of personal data for direct marketing purposes and the processing of personal data resulting in automated decision making.[578]

---

570 The subsequent use of private facts acquired by a wrongful act of intrusion remains unlawful (see par 2.3.2.2). This reflects the data protection principle of fair and lawful processing (see ch 6 par 2.2.1).

571 This include natural and juristic persons.

572 This is a reflection of the data protection principle of openness (see ch 6 par 2.2.7).

573 This is a reflection of the data protection principle of openness (see ch 6 par 2.2.7).

574 This reflects the data subject participation principle (see ch 6 par 2.2.6).

575 This is a reflection of the data protection principle of openness (see ch 6 par 2.2.7).

576 This reflects the data subject participation principle (see ch 6 par 2.2.6).

577 This reflects the sensitivity principle (see ch 6 par 2.2.8).

578 See ch 6 par 2.2.6.

(f) Reasonable security measures must be taken by the data controller to secure the integrity and confidentiality of the data.[579]

(g) (i) The data controller should be held accountable for implementing the data protection principles.[580]

(ii) It is a defence against a delictual claim by the data subject that the data controller took all reasonable steps to comply with the data protection principles; or that non-compliance with the principles was due to *vis major* or the fault of the data subject.[581]

(iii) Fault is not required for the delictual liability of the data controller for the patrimonial and non-patrimonial loss of the data subject.

(h) Exceptions and exemptions from these principles may be provided for where the risks to the privacy or identity of the data subject are relatively small or where other interests (public interests, interests of other parties or those of the data subject him- or herself) override the data subject's rights to privacy or identity.[582]

579 See also Burchell *Personality rights* 399. This relates to the principle of security and confidentiality (see ch 6 par 2.2.9).

580 This reflects the accountability principle (see ch 6 par 2.2.10).

581 See text to fn 472.

582 See par 2.3.2.3 .