BILETA
British & Irish Law, Education and Technology Association
2007 Annual Conference
Hertfordshire 16-17 April
UH

Blowing the whistle on Sarbanes-Oxley: Anonymous hotlines and the historical stigma of denunciation in modern Germany

Judith Rauhofer
Law tutor, University of Liverpool
Email: J.Rauhofer@liverpool.ac.uk

Abstract:

The Sarbanes-Oxley Act requires listed US companies as well as non-US companies listed on a US stock market to establish procedures for dealing with confidential, anonymous employee submissions regarding questionable accounting or auditing matters. Companies failing to comply with these "whistleblowing" requirements are subject to heavy sanctions. This paper examines the compatibility of whistleblowing requirements contained in the US Sarbanes-Oxley Act with EU data protection rules, and analyses the roots of the historical unease with and the stigma attached to whistleblowing schemes in Germany which result from its experiences with denunciation during the Third Reich and in the former GDR.

1. Introduction

In August 2001, Sherron Watkins, vice-president for corporate development at Enron Corporation, then one of the world's leading energy and communications companies, alerted Enron's Chairman and CEO, Kenneth Lay, in an anonymous memo to certain accounting improprieties committed by the company's senior staff and its accounting firm Arthur Andersen. In October 2001, the US Securities and Exchange Commission (SEC) announced that it had begun an inquiry into Enron's accounting and auditing practices which later developed into a a formal investigation. Enron was found to be in breach of a number of accepted accounting standards and filed for bancruptcy in December 2001. Arthur Andersen voluntarily surrendered its accounting licence in 2002, thereby effectively dissolving its partnership.

When asked why she had not reported her observations earlier to her immediate superior or the company's CEO, Sherron Watkins replied that she „was not comfortable confronting either [of them] with [her] concerns. To do so, [she] believed, would have been a job-terminating move"[1].

As the Enron and other high profile corporate scandals sent shock waves through stock exchanges the world over, public confidence in accepted reporting and accounting practices declined. This prompted the US administration to review its regulatory framework for corporate governance and on 30 July 2002 the US Congress adopted the Public Company Accounting Reform and Investor Protection Act of 2002, commonly known as the Sarbanes-Oxley Act 2002 (SOX). SOX established new or enhanced standards for all US public company boards, management, and public accounting firms. The Act contains 11 titles, or sections, ranging from additional Corporate Board responsibilities to criminal penalties, and requires the SEC to implement rulings on requirements to comply with the new law.

Sherron Watkins' role in revealing the failure of the corporate governance structures almost directly resulted in some of the new provisions contained in SOX, including a requirement for listed companies to establish corporate codes of ethics regulating the conduct of senior financial officers and a requirement to put in place internal reporting structures which allow employees to bring accounting and auditing irregularities to the attention of senior managers anonymously and without fear of retribution.

However, US public companies faced significant difficulties when trying to introduce the same "ethics" codes, backed up by anonymous hotlines, at their European subsidiaries. In 2005 the French data protec-

[1] Testimony of Sherron Watkins before the Oversight and Investigations Subcommittee of the House Energy and Commerce Committee on the financial collapse of the Enron Corporation, as recorded by the Feral News Service, available at http://www.apfn.org/enron/watkins2.htm, last accessed on 30 November 2006

tion authority, the "Commission national de l'informatique et des libertés" (CNIL), prevented a French subsidiary of McDonalds from establishing anonymous whistleblowing procedures on the grounds that it involved the transfer of personal data of the person accused of wrongdoing. CNIL argued that EU data protection law prevented the transfer of data without the data subject's consent. It also refused to authorize another "ethics hotline" put into place by a subsidiary of US technology company, Exide Technologies[2]. Around the same time, a German employment court held that substantial parts of the code of conduct US retailer Wal-Mart wanted to introduce for its German subsidiary were invalid under German law[3].

It has been argued that the attitude of the French and German authorities in these cases is influenced by a deep cultural unease about the concept of whistleblowing itself. Both countries have experienced in their history how the ability of individual citizens to provide information to those in authority, allegedly for the purpose of protecting a higher common good, has been abused by those individuals for their own selfish motives. Germany, in particular, still suffers from its dual experience of mass denunciations during the Hitler regime and in the former GDR. The latter regime, in the form of its Ministry for State Security, heavily relied on the information provided by a network of so called "Inofficial Contributors" for the establishment of a system of almost total surveillance and control of its populace. A feeling therefore seems to dominate which likens the act of "blowing the whistle" to that of denunciation, with the latter being tarnished with considerable social and historical stigma.

US based companies that fail to comply with the whistleblowing requirements set out in SOX are subject to heavy penalties[4]. Those same companies are facing risks of sanctions from EU data protection authorities and the national courts of EU member states if, when establishing US style whistleblowing schemes, they fail to comply with EU data protection rules and national constitutional and employment laws. This has led to a situation where companies will be "damned if they do and damned if they don't".

This paper will examine the compatibility of SOX with the EU data protection regime and German employment and constitutional legal framework. It will consider the way in which the moral and legal sensibilities which result from Germany's historical experiences inform the way in which it views and regulates whistleblowing schemes. The paper will argue that individual rights and freedoms, such as the personality right protected in Article 2 of the German Constitution (GG) provide a constitutional framework largely designed to allow for the protection of the person accused of wrongdoing rather than the whistleblower.

2. The requirements of the Sarbanes-Oxley Act

SOX is one example of the „codification" of the process of whistleblowing for defined public good purposes.

2.1. Codes of ethics or conduct

Section 406(a) SOX requires public companies to adopt a „code of ethics" for senior financial officers or persons performing similar functions which must include standards necessary to promote:

- "honest and ethical conduct, including the ethical handling of actual or apparent conflicts of interest between personal and professional relationships;
- full, fair, accurate, timely, and understandable disclosure in the periodic reports required to be filed by the issuer; and
- compliance with applicable governmental rules and regulations."[5]

Similar provisions are included in the regulations enacted by the two biggest US stock exchanges, NASDAQ and NYSE, which also require companies listed in those markets to adopt corporate govern-

---

[2] CNIL Decision 2005-110 of 26 May 2005 (Group McDonald's France) and CNIL Decision 2005 2005-111 of 26 May 2005, English translations available at http://www.theworldlawgroup.com/newsletter/details.asp?ID=1243487122005 and http://www.theworldlawgroup.com/newsletter/details.asp?ID=1246367122005, last accessed on 30 November 2006.

[3] ArbG Wuppertal on 15.6.2005, 5 BV 20/05, NZA-RR 2005, 476. This decision was later confirmed on appeal, LAG Düsseldorf on 14.11.2005, 10 TaBV 46/05, BB 2006, 335 = NZA-RR 2006, 81. Wal-Mart has appealed the decision to the Federal Emploment Court (reference 1ABR 1/06) but a decision is still outstanding.

[4] See infra, paragraph 2.2.

[5] Section 406 (c) SOX

ance guidelines or codes of conduct applicable to senior financial officers and directors, in relation to accounting, reporting and auditing matters[6].

2.2. Putting in place a complaints procedure

Under section 301(4) SOX the audit commission of each public company governed by the Act must put into place "procedures for the receipt, retention, and treatment of complaints received by the [company] regarding accounting, internal accounting controls, or auditing matters and the confidential, anonymous submission by employees of the [company] of concerns regarding questionable accounting or auditing matters".

While no particular complaints procedure is prescribed and while companies can "provide for a variety of employee reporting methods"[7], section 301 SOX requires that "at least one confidential, anonymous method is available to employees"[8].

Each code of coduct adopted under the relevant rules of the NYSE and NASDAQ must contain an enforcement mechanism that ensures prompt and consistent enforcement of the code, clear and objective standards for compliance, and a fair process by which to determine violations[9]. The facilitation of whistleblowing by employees forms part of the enforcement strategy used by many companies, as complaints or alerts from the inside are seen as the most efficient way to ensure that "ethics are valued within an organisation and potential issues are surfaced to the right supervisor and even management to deal with them as soon as they arise."[10].

Companies which fail to comply with these requirements may face SEC civil penalties and/or, in extreme case, the de-listing from the stock exchange on which their shares are traded[11].

2.3. Protecting employees from retribution

Section 806 SOX provides protection for whistleblowing employees from retaliatory measures taken against them by making it illegal for companies to "discharge, demote, suspend, threaten, harass, or in any other manner discriminate against" such employees for reporting accounting irregularities or for assisting the relevant government and regulatory agencies in their inquiries into such irregularities. Employees who allege discrimination or termination of their employment agreement because of their involvement in an enquiry have the right to file a complaint with the US Secretary of Labor and, if the Secretary has not issued a final decision on that complaint within 180 days, to bring an action in court against their discriminatory treatment or dismissal.

These employee protection rules were clearly designed to overcome the fear of potential whistleblowers that their actions might result in their immediate dismissal[12]. However, the concept itself is by no means new to Anglo-American law as it has also been employed in the other Acts which were designed to encourage informing by private individuals on the actions and behaviour of fellow citizens[13].

3. The nature of whistleblowing

---

[6] See, for example, NYSE Listed Company Manual, section 303A(9) and NASDAQ Rule 4350(n).
[7] id., p.V-9-7.
[8] Schreiber et al, P. V-9-7
[9] See, for example, NASDAQ Rule IM-4350-7
[10] Schreiber et al. (2006), p. V-9-4
[11] Section 20 Securities Exchange Act of 1934
[12] See note 1 supra.
[13] Other examples include the US False Claims Act designed to protect employees who blow the whistle on the unlawful obtaining and use by their employees of public monies and the UK Pulic Interest Disclosure Act 1998 under which any employee who is dismissed for reporting similar offences by his employer can be awarded unlimited damages, Schreiber, M.E; Held, J.E; Bond, R.T.J.; Dan, R.;Runte,C. and Flower, K. (2006) "Anonymous Sarbanes-Oxley Hotlines for Multi-National Companies: Compliance with EU Data Protection Laws" in The Practitioner's Guide to the Sarbane-Oxley Act, Volume II, American Bar Association, p. V-9-26.

Near and Miceli define the term “whistleblowing” widely as „the disclosure by organisation members (former or current) of illegal, immoral, or illegitimate practices under the control of their employers, to persons or organisations that may be able to effect action”[14].

3.1. The whistleblower as an „insider”

The whistleblower’s position as an organisational insider is is a key factor in determining the protection he deserves[15]. Only persons who have a close connection with the organisation whose wellbeing is threatened by the practice they seek to expose will themselves be at risk of being affected either by the practice itself or by its disclosure. Mere rumours spread by unrelated third parties about certain individuals will rarely assist the management of the relevant organisation in addressing truly pressing issues of corporate governance.

3.2. Illegal or unethical practice

The procedure which is exposed by the whistleblower must be in some form illegal. It must be capable of harming the relevant organisation, its employees (including, possibly, the whistleblower) and/or a public or common good. In the case of accounting improprieties, for example, it is acknowledged that the consequences of such improprietes harm investor confidence in accepted accounting procedures. This could have a negative impact on share prices and investor behaviour in general.

However, difficulties arise in relation to legal but merely unethical conduct. Although social scientists seem to assume that the act of whistleblowing is always “morally desirable”[16], one could argue that the morality of the act is dependent on the legitimacy of the behaviour the act seeks to uncover. As Near and Miceli point out, the illegitimacy of the activities of an organisation or individual members of an organisation “is in the eye of the beholder, namely the whistleblower”[17]. They argue therefore that the concept of legitimacy, in the Weberian sense of activities which organisations have the authority to commit, is crucial in this context. According to Weber, the basis of such authority is the acceptance by organisation members and society that such actions are appropriate[18].

However, historical experience, for example during the NS-Regime, shows that individuals who informed on neighbours and colleagues for offences against the regime felt entirely justified in their belief that their actions benefited the public good[19] and that the behaviour of those they accused of wrongdoing fell foul of their concept of legitimacy. The values those informers sought to protect, for example racial purity, obedience to the ruling government etc., while commonly accepted by members of German society at the time, were not, in many cases, values which would be upheld by today's constitutional democracies. Whistleblowing must therefore be seen in the context of the legal and ethical framework in which it occurs.

If one defines ethics as the “human concern for the degree of rightness involved in making intentional and voluntary choices in conduct touching on such moral values as justice, goodness and truthfulness, and which carries the potential for significantly affecting other people”[20] individuals, when making ethical choices, are guided by a variety of standards based on, among other things, the political values of their nation, their religious admonitions[21], legal regulations, the utilitarian perspective (greatest good for the

---

[14] Near, J.P. and Miceli N.P. (1985) “Organisational dissidence: the case of whistle blowing”, Journal of Business Ethics, Vol. 4 pp.1-16. For an excellent description of the three elements, see Hoppler, B. (2005) “Whistleblowing – ein integraler Bestandteil effektiver Corporate Governance”, BB 2005 Vol. 48, p. 2623

[15] Hoppler, B. (2005), p. 2623

[16] Brinker Dozier, J. and Miceli, M.P. (1985), p. 827

[17] Near, J.P. et a. (1985), p. 3

[18] Weber, M. (1947) “The theorie of social and economic organisation”, Free Press, New York

[19] See, for instance, the case of Helene Schwärzel who reported Dr. Carl Goerdeler, a former mayor of Leipzig and one of the conspirators in volved in the July plot which aimed to assassinate Hitler as described in Sauerland, K. (2000) “30 Silberlinge_ Denunziation – Gegenwart und Geschichte”, Verlag Volk & Welt, Berlin, pp. 13-15

[20] Jensen, J.V. (1987), p.321-322

[21] For example: in a study by Barnett, Bass and Brown examining the relationship between religiosity and ethical ideology and ethical ideology and ethical judgements about and intentions to report peer wrongdoing, subjects were asked to read a vignette concerning academic cheating and to respond to certain “ethical” questions about the vignette. Results indicated that religiosity was positively associated with an ethical ideology of non-relativism. Individuals whose ethical ideologies could thus be described as idealistic and non-relativistic were more likely to state that reporting a peer's cheating was ethical. In turn, individuals who believed reporting a peer's cheating was ethical were more likely to say that they would report a peer's cheating, see Barnett, T., Bass, K. and Brown, G.)1996) “Religiosity, Ethical Ideology, and Intentions to Report a Peer's Wrongdoing”, Journal of Business Ethics 15, pp. 1161-1174.

greatest number) as well as some situational guidelines[22]. It is clear, therefore, that any concept of "legitimacy" is vulnerable to personal bias as well as social, political and historical change. In extreme cases this can lead to an unfair accusation of individuals who, for some reason, deviate from the accepted norm notwithstanding the fact that the "ethics pedigree" of that norm itself may be questionable.

3.3. Report to a person in a position to take action

Whistleblowing is usually defined as the reporting of certain behavior in disregard of an organisation's accepted line management structures[23], since the whistleblower is necessarily an individual who lacks a legitimate power base to change the organisation's acitivities and who must therefore rely on other informal bases of power[24].

The reasons for the circumvention of such structures are manifold and include not only the mistrust of one's immediate line manager or the believe that they will not take action, but also the fear of retribution, the need for anonymity or – on the contrary – the wish to be recognised for one's actions by someone in the organisation's „higher order". Near and Miceli have argued that the initial reluctance of some organisations to establish systems which protect whistleblowers from retribution may be attributed to this circumvention of established authority structures. While the whistleblower may provide valuable information helpful in improving the organisation's effectiveness or in detecting the prevalence of illegal activity, publicly condoning a challenge of that structure may "push the organisation into chaos and anarchy"[25].

Different opinions are voiced in the relevant literature on the required status of the person to whom the offending behavior is reported. Some authors argue that whistleblowing only occurs when the accuser involves persons external to the affected organisation[26]. However, this school of thought seems contrary to the Anglo-American understanding of whistleblowing as a process which primarily concerns the affected organisation, its officers and its other members (for example, employees). A wider definition of whistleblowing which disregards the question of whether the person to whom the report is made is an insider or external to the organisation therefore seems more appropriate.

3.4. Whistleblowing as a form of pro-social behaviour

In assessing the legitimacy of whistleblowing arrangements it is important to consider the whistleblowers' motives. Brinker Dozier and Miceli argue that while whistleblowing is not an act of pure altruism, defined by Batson as a „desire of one organism to increase the welfare of another as an end-state goal"[27], it is nonetheless „a form of pro-social behaviour"[28], involving both „selfish (egoistic) and unselfish (altruistic) motives on the part of the actor". According to Staub, pro-social behaviour is positive social behaviour that is intended to benefit others[29]. However, pro-social actors can also intend to gain rewards for themselves, so that in some cases, whistleblowers might seek personal advantages from their behavior. As the degree to which people intend to benefit themselves by benefiting others varies across instances of pro-social behaviour, Staub argues that it is not necessary for unselfish motives to dominate. They must simply be present and contribute to the individual's urge to take action.

One could argue that in case of a genuine violation of an organisation's accepted standards, it is irrelevant if the whistleblower's actions are also informed by selfish motives. But (co-)existence of selfish and altruistic motives both, raises the spectre of a possible abuse of process and could also make unjustified whistleblowing more likely. It has been well established that a large proportion of informants' reports dur-

---

[22] Johannesen, R.L. (1983) "Ethics in Human Communication", 2nd ed., Waveland Press, Prospects Heights

[23] See, for example, the definitions used in Leisinger, (2003) "Whistleblowing und Corporate Reputation Management", Rainer Hampp Verlag, Mering, pp. 27-29

[24] Elliston, F.A. (1982) "Anonymity and whistleblowing", Journal of Business Ethics 1, pp 167-177

[25] Near, J.P. and Miceli, M.P. (1985) "Organizational Dissidence: The Case of Whistle-Blowing", Journal of Business Ethics 4, pp. 1-16

[26] See, for example, Jubb, P.B. (1999) "Whistleblowing: A Restrictive Definition and Interpretation", Journal of Business Ethics , Vol. 21, pp. 77-94

[27] Batson, C.D. (1983) "Sociobiology and the role of religion in promoting prosocial behavior: An alternative view", Journal of Personality and Social Psychology, 45, 1380-1385

[28] Brinker Dozier, J. and Miceli, M.P. (1985) "Potential Predictors of Whistleblowing: A Prosocial Behavior Perspective", Academy of Mangement Review, Vol. 10, No 4, pp.823

[29] Staub, E. (1978) "Positive social behavior and morality: Social and personal influences" Vol. 1, New York, Academic Press,

ing both the NS-Regime and in the former GDR was motivated by personal differences with the object of the denunciation. Many people were moved to their actions by a desire to cause damage to the reputation of a superior or a wish for revenge. Many sought "self-aggrandisement and publicity"[30] or acted because it provided them with a feeling of power or the illusion of participating in and supporting executive control. Often reports were made by the socially weaker party against the stronger[31]. At the same time, the habitual reporting of minor rule violations, largely for selfish reasons, may lead to a shift in the organisation's social climate. Consequently, one must question Staub's contention that whistleblowing behaviour can be classified as pro-social even if it is not the altruistic motive which dominates the action.

3.5. Anonymity and whistleblowing

The question whether whistleblowing should be done anonymously or openly will significantly influence the way in which the practice is viewed by society. Jensen points out that engaging in whistleblowing openly tends to create greater credibility, since the person "exhibits great courage in courting considerable punishment from the organisation"[32]. On the other hand, keeping one's idenity secret "carries with it more protection, and may embolden the whistleblower to be more comprehensive and incisive, thus getting to the heart of the case more quickly and more effectively"[33]. The question arises how fair it is to the public, and to the person accused of wrongdoing, not to know the source of the charges? Does the latter have the right to know the whistleblower's identity or do they have the right to withhold it?

The reason generally given for allowing whistleblowers to remain anonymous is that they must be protected from retaliation by the organisation or the individual whose activities they report. Elliston therefore proposes that the greater the probability of unfair retaliation, the weaker the prohibition on anonymity should be.

On the other hand, anonymity may be condemned because it impedes the pursuit of truth. Whistleblowers who level accusations against another while remaining anonymous makes it more difficult, albeit not usually impossible, to determine whether their charges are true or false. Because they cannot be questioned or asked for their sources of information, their accusations are harder to verify or to repel.

Elliston has likened anonymous whistleblowig to a "paradigm of bad manners", allowing the whistleblower "to say nasty things about people not present to defend themselves"[34]. He argues that the reason for this harsh condemnation of the practice can be found in the concept of loyalty in that "[t]o be a faithful member of a group is to protect the interests of that group as a whole and of its members individually."[35] Many whistleblowers will indeed experience moral conflict if they feel that their inclination to act might lead to a violation of fundamental norms of their reference groups[36]. As Bok argues:

"Conflict between responsibilities is reflected in conflicting messages within many professions: The professional ethic requires collegial loyalty, while the codes of ethics often stress responsibility to the public over and above duties to colleagues and clients[37]."

It is clear, however, thar accusing other members of a group behind their backs has the potential to disrupt the cohesion of the group, undermine trust in each other and threaten group solidarity.

In addition, whistleblowers may use their anonymity to hide their own selfish motives for their actions. If they cannot be traced, they cannot be held accountable for wrong and unfair accusations, at least not by the person against whom their allegations are directed. One must therefore distinguish between " reasons and causes, the justification and the motivation, the evidence that proves a statement true or false and the personal considerations that lead a person to utter it"[38]. Where accusations are incorrect or made in

---

[30] Bok, S. (1980) "Whistleblowing and professional responsibilities" in P. Callahan and S. Bok (Eds.) "Ethics Teaching in Higher Education", pp. 277-295
[31] Sauerland, K. (2000), p. 53
[32] Jensen, J.V. (1987) "Ethical Tension Points in Whistleblowing", Journal of Business Ethics 8, pp. 321-328
[33] id.
[34] Elliston (1982), p. 171
[35] id.
[36] Schwartz, S.H., Feldman, K.A., Brown, M.E. and Heingartner, A. (1969) "Some personality correlates in personal conduct in two situations of moral conflict", Journal of Personality 37, pp. 41-57
[37] Bok, S. (1980), pp. 277-278
[38] id.

bad faith, granting a whistleblower anonymity will add to the problem that the system may be abused by individuals for their own self-interest.

4. The compatibility of whistleblowing rules with the EU data protection regime

The reporting by a whistleblower of a specific individual for perceived violations of rules such as a company's code of ethics will necessarily entail the collection of certain information about that individual. If such information can be categorised as „personal data", the collection of that data by an organisation and the further transfer of such data to associated or external organisations within or outside the EU must be compliant with EU data protection rules.

4.1. The EU data protection regime

The processing of personal data inside the European Union and the transfer of such data from the EU to countries outside the European Economic Area (EEA) is subject to the data protection regime set out in Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the Data Protection Directive)[39]. The Directive introduced broad obligations on those who collect personal data (data controllers[40]), as well as conferring broad rights on individuals about whom data is collected (data subjects[41]). „Personal data" is defined in Article 2(a) of the Directive as information relating either to an identified person or a person who can be identified, directly or indirectly, by reference to a reference number or by one or more factors specific to him.

4.1.1. Legitmacy of whistleblowing schemes

According to Article 6 of the Data Protection Directive, personal data must be provided „fairly and lawfully". For a whistleblowing scheme to be lawful, the processing of personal data carried out as part of the procedure must be legitimate, and satisfy one of the grounds set out in Article 7 of the Directive. These grounds include, among other things, situations where:

- The processing is necessary for compliance with a legal obligation to which the data controller is subject42. This could arguably include a company's obligation to comply with the provisions of SOX.
- The processing is necessary for the purposes of the legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests or the fundamental rights and freedoms of the data subject which require protection under Article 1(1) of the Directive. Again, one could argue that the SOX requirement to establish reporting systems may be found necessary for the purposes of a legitimate interest pursued by the company establishing those systems or by a third party, including the US parent company and the US regulator, to whom the data are subsequently disclosed.

4.1.1.1. Compliance with a legal obligation

A certain amount of uncertainty exists about whether or not all of the SOX provisions apply to companies established outside the US. In January 2006, the US Court of Appeals held that the provisions on the protection of whistleblowers contained in section 806 SOX do not apply to foreign citizens working outside the US for foreign subsidiaries of US companies[43]. Although this is only a 1st Circuit decision which is currently under judicial review, it has raised questions over the general applicability of SOX in Europe.

However, as sections 301 and 406 clearly seem to apply to multi-national companies, Schreiber et.al. conclude that the limitation of the extra-territoriality of individual rights under section 806 does not seem to affect the extra-territoriality of the requirements of establishing a code of conduct and/or a related complaints procedure[44].

---

[39] OJ L281/31
[40] Article 2(d) of the Data Protection Directive
[41] Article 2(a) of the Data Protection Directive
[42] Article 7(c) of the Data Protection Directive
[43] Carnero v. Boston Scientific Corp., 433 F.3d 1, 87 Empl. Proc. Dec. P 42, 193, 23 IER Cases 1505 (1st Cir. 2006)
[44] Schreiber et.al. (2006), p. V-9-8

Regardless of the question of applicability, however, the EC Article 29 Working Party, in its opinion on the compatibility of whistleblowing schemes with EU data protection rules[45], has concluded that in any case „an obligation imposed by a foreign legal statute or regulation [...] may not qualify as a legal obligation by virtue of which data processing in the EU would be made legitimate" as „[a]ny other interpretation would make it easy for foreign rules to circumvent the EU rules laid down in [the Data Protection Directive]"[46]. As a result, SOC whistleblowing provisions may not be considered as a legitimate basis for processing on the basis of Article 7©"[47].

4.1.1.2. Processing for the purpose of legitimate interests of the controller

The Article 29 Working Party has acknowledged that whistleblowing schemes adopted to ensure the stability of financial markets and the „prevention of fraud [...] as well as the fight against bribery, banking and financial crime, or insider trading" might be seen as serving a legitimate interest of a company that would justify the processing of personal data by means of such schemes. The need of subsidiaries of US companies or non-US companies listed at US stock exchanges to comply with the US regulatory framenwork can also be seen as a legitimate interest of such companies.

However, as the Working Party points out in its opinion, Article 7(f) of the Directive requires „a balance to be struck between [that legitimate interest] and the fundamental rights of data subjects"[48]. The Working Party argues that, in accordance with Article 6 of the Directive, „this balance of interest test should take into account issues of proportionality, subsidiarity, the seriousness of the alleged offences that can be notified and the consequences for the data subjects"[49]. It particular, „adequate safguards" would have to be put into place as well as provisions safeguarding the data subject's right under Article 14 of the Directive „to object at any time on compelling legitimate grounds to the processing of the data relating to them".

4.2. The recommendations of the EC Article 29 Working Party on establishing compatible codes of conduct[50]

Based on its assessment of the compatibility of whistleblowing schemes with EU data protection rules, the Working Party made a number of recommendations.

The working party considered that the application of the principles of data quality and proportionality[51] had a number of consequences for whistleblowing schemes:

- It suggested that in application of the proportionality principle, the company responsible for the whistleblowing scheme should carefully assess whether it might be appropriate to limit both the number of persons eligible for reporting alleged misconduct and the number of people who might be incriminated, in particular in the light of the seriousness of the alleged offences, although it acknowledged that in both cases the categories of personnel involved may still "sometimes include all employees in the fields of accounting, auditing and financial services"[52].

---

[45] Article 29 Working Party Opinion 1/2006 on the application of EU data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime, WP 117, 1 Februar 2006 (Article 29 Working Party Opinion)

[46] id., p. 8

[47] The Working Party does acknowledge that principles and guidelines have been developed by international organisations such as the OECD and the EU which "recognise the importance of relying on good governance". It also recognises that some EU member states, such as Spain and the Netherlands, have themselves adopted regulations requiring whistleblowing schemes to be put into place and that such regulations would, of course, be seen as a legally binding obligation on the data controller which would permit him to collect the relevant personal data under Article 7(c) of the Directive.

[48] Article 29 Working Party Opinion, p.9

[49] id.

[50] The Working Party's recommendations bear close resemblance to a set of Guidelines issued by the French data protection authority, CNIL, in November 2005 which provided a "pragmatic and practical approach, allowing US and other companies operating in France a specific framework for dual compliance" (see Schreiber et.al. (2006), p. V-9-11). An English version of the Guideline is available at http://www.cnil.fr/fileadmin/documents/uk/CNIL-recommandations-whistleblowing-VA.pdf, last accessed on 1 December 2006. Due to the obvious constraints, this paper will not be able to analyse these Guidelines in more detail.

[51] Article 6 Data Protection Directive

[52] Article 29 Working Party Opinion, p. 10

- The Working Party pointed out that although in many cases, anonymity of complaints was desirable, if not necessary to achieve the specified aims, where possible, whistleblowing schemes should be designed in such a way that they did not encourage anonymous reporting as the usual way to make a complaint. Rather, reporting should be identifiable but confidential[53]. The Working Party argued that there were a number of practical reasons as to why anonymous reporting was not always desirable, including the fact that it made it harder for investigators to contact the whistleblower for follow-up questions and the fact that it was easier to organise protection of the whistleblower (whose identity might, in any case be guessed by his co-workers) against retaliation. A scheme promoting anonymous reports, on the other hand, would run the risk of negatively affecting the social climate within an organisation which, in turn, might result in „developing a culture of receiving anonymous malevolent reports" or might "lead people to focus on the whistleblower, maybe suspecting that he or she is raising the concern maliciously"[54]. The Working Party also suggested that only identified reports would satisfy the requirement that data be collected fairly.

- The Working Party recommended that the type of information to be collected and processed through the scheme should be defined and limited to accounting, auditing and related matters[55]. The personal data processed within the scheme should be limited to the data strictly and objectively necessary to verify the allegations made, and data should, where possible, be deleted within two months of the end of an investigation.

- The Working Party reminded companies that as data controllers they must provide information about the existence, purpose and operation of the scheme to the data subject under Article 10 of the Directive[56].

- The Working Party noted that it was essential to balance the rights of the person incriminated, the whistleblower and the company's legitimate investigation needs. In accordance with Articles 11 and 14 of the Directive, an accused person should be informed as soon as possible of the matters of which they were accused, details relating to the scheme, and their rights to access the data and to have it rectified or erased in the event of error. In no circumstances should the identity of the whistleblower be disclosed unless there were grounds for believing that the accusation had been made maliciously. At the same time, the Working Party acknowledged that in some cases, granting data subjects access to the information collected about them, might jeopardise the company's ability effectively to investigate the allegations made, or to collect the required evidence. In this case, the Working Party agreed that "notification to the incriminated person [might] be delayed as long as such risk exists"[57].

- The Working Party set out several guidelines as to how a whistleblowing scheme should be managed. It recommended that, internally, a dedicated investigation group should be established, separate from other departments of the company, dedicated to handling whistleblowers reports and leading the investigation. It should consist of a limited number of specially trained people who would be bound by confidentiality obligations. Any external bodies involved in the scheme should also be bound by terms of confidentiality. Moreover, the Working Party believes that, as a rule, multi-national groups should deal with reports locally, i.e. in the (EU) country where the complaint is filed, rather than „automatically share all the information with other companies in the group"[58].

- The Working Party stated that, in accordance with Article 25 of the Data Protection Directive, data should only be transferred to a third party outside the EU where that country ensures an adequate level of protection. If the transferee was an entity established in the US, currently only the "Safe Harbor" scheme provided for an adequate level of protection for data transfers from the EU to US organisations which have joined the scheme. Where companies had not, or could not[59], join the Safe Harbor scheme, they

---

[53] id.
[54] id. p.11
[55] id., p.12
[56] id., p.13
[57] id., p.13
[58] id. This should also assist in achieving compliance with Article 25 of the Directive as it minimises the possibility that personal data of EU citizens are transferred to countries outside the EEA, see paragraph **Error! Reference source not found.**infra.
[59] Note that the Safe Harbor scheme does not apply to financial services so that this would automatically exclude some US or US listed companies from following this route.

had to rely on other safeguards such as entering into a data transfer contract with the EU entity, for example based on the standard contract clauses issued by the European Commission in its Decisions of 15 June 2001 or 27 December 2001 and 7 January 2005[60] or by relying on a set of binding corporate rules put in place by the group to which both companies belong with the aim of facilitating group-internal cross-border data transfers and which the competent data protection authorties had approved.

5. The compatibility of whistleblowing rules with German law

As shown above, there exists a fundamental difference between the perception of a whistleblowers' role and status in society in the Anglo-American jurisdictions and those of Continental Europe, specifically Germany.

5.1. The historical stigma of denunciation in Germany

Although so far, only a small number of whistleblowing cases have been decided by the German courts[61] many of those decisions seem to mirror the famous remark by Hoffman v. Fallersleben[62] that the informer is "the greatest villain in the land"[63]. This reflects an attitude which sees the informer as someone who "befouls their own nest"[64], particular where information about another person is passed on to the state. Müller has argued that this attitude is partly due to the fact that, in Germany since the days of the liberation movement in the early 19th century, the state has never been understood as an entity made up by and representing its citizens (as in the United States). Rather that the image of the authoritarian state with which no solidarity can exist remains prevalent in peoples' minds.[65] It is submitted, however, that in view of the undeniable democratisation of the public consciousness since the end of Worl War II, this argument is fast loosing credibility. A better explanation for the German approach to whistleblowing might be that it is – still - informed by and reflects a deep historical unease about a form of „personal activism" so reminiscent of behavior that was widely used (and abused) in Germany's most recent past.

Denunciations during the NS-Regime grew from relatively small beginnings to a situation where fear and distrust became the norm in German society. In many cases denunciations were used to bring "deviating behaviour" (such as homosexuality or relationships between Germans and members of other "races") to the attention of the police and the security services. Towards the end of the Third Reich, the majority of criminal prosecutions for certain offences, for example violations of the laws angainst racial purity, can be traced back to reports by third party informers.[66] The regime had declared that German citizens had a moral obligation "actively to contribute to national and public security and the united […] national community[67] by reporting "moaners" and "defeatists" who criticised the system or the government. Although the image of the Gestapo as omnipresent, omnipotent and omniscient still prevails, studies have shown that in light of the task it was set, it was in fact "understaffed and overbuerocratic"[68]. Before the annexion of Austria in 1938, only around 7,000 persons were employed by the Gestapo, only about half of them were in active police service. At the end of 1944 the service employed approx. 32,000 people in all of Germany including the occupied territories. In 1937, in Düsseldorf, then a town of approx. 650,000 inhabitants,

---

[60] Decision (2002/16/EC) of 27 December 2001 on standard contractual clauses for the transfer of personal data to third countries under the Directive (OJ 2002 L6/52); Decision 2001/497/EC of 15 June 20021 on standard contractual clauses for the transfer of personal data to third countries under the Directive (OJ 2001 L181/19); and Decision 2004/915/EC of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries (OJ 2004 L385/74).

[61] See Graser, D. (2000) "Whistleblowing – Arbeitnehmeranzeigen im US-amerikanischen und deutschen Recht", Europäiche Hochschulschriften, Frankfurt am Main/Wien, p. 181; Graser only list four decisions of the Federal Employment Court (BAG) which deal with the legality of whistleblowing in an employment context.

[62] (1798-1874)

[63] "Der größte Lump im ganzen Land – das ist und bleibt der Denunziant"

[64] "Nestbeschmutzer"

[65] Müller, M. (2002) "Whistleblowing – ein Kündigungsgrund?", Neue Zeitschrift für Arbeitsrecht (NZA), pp. 428-437

[66] Rüping, H. (1997) "Denunziation und Strafjustiz im Führerstaat" in Jerouschek, G., Marßolek, I., Röckelein, H. (eds.) "Denunziation: Historische, juristische und psychologische Aspekte", edition discord, Tübingen, pp. 127-145

[67] Diewald-Kerkmann, G. (1997) "Politische Denunziation im NS-Regime", in Jerouschek, G. et al. (eds.), pp. 146-156

[68] Mallmann, K.M., Paul, G. (1993) "Allwissend, allmächtig, allgegewärtig? Gestapo, Gesellschaft und Widerstand" in Zeitschrift für Geschichtswissenschaft 41, 11, p. 989

there were only 126 active members of the Gestapo[69]. Mallmann and Paul conclude that "without the army of willing informers, the Gestapo would have been effectively blind"[70].

Informers were used by the regime for the purpose of social control and to impose and enforce its own political ideas. However, while it is often assumed that informers did what they did because they were afraid for their personal safety, studies have shown that political denunciations were more often motivated by personal reasons, petty disagreements and an unhealthy tendency towards improving one's one image with the authorities[71]. Even Hitler himself acknowledged this when he observed that "we currently live in a sea of denunciations and human meaness" where individuals frequently informed on another person while recommending themselves as their successor[72]. Many denunciation led to prosecutions before the German Special Courts and the imposition of severe penalties against those accused of deviance or wrongdoing.

Only a few decades later, the communist regime in the former GDR employed similar methods when it set up the Ministry for State Security ("Stasi") which used a network of "Inofficial Contributors", most of them neighbours, family members or co-workers of those on whom they informed. This network played a major part in turning the GDR into what the West German media later described as "the most perfected surveillance state of all time". Official statistics show that at the end of the regime the Stasi had 97,000 employees to oversee a country of 17 million people. This would mean that there was one Stasi officer for every 175 people. By comparison, it is estimated that in Hitler's Third Reich there was one Gestapo agent for every 2000 citizens, and in Stalin's USSR there was one KGB agent for every 5830 people[73]. However, the Stasi is also reported to have had 174,000 inofficial contributors among the population[74]. This would bring the ratio of observers to citizens down considerably, making it one Stasi officer or informant for every 63 people.

Many explanations have been found for this willingness of the German people to inform on their fellow countrymen and women, from fear of Stasi retribution to "an impulse to ensure that your neighbour was doing the right thing" often linked to the "German mentality" which is alleged to include "a certain drive for order and thoroughness"[75]. One major difference between Stasi inofficial contributors and Gestapo informers can be seen in the way in which they became active. While during the Nazi-Regime informers often reported events and third party actions voluntarily and for their own personal motives, Stasi collaborateurs were recruited by Stasi officers. Recruitment was seen by the recruited as either a threat or an "act of trust" by the state. In the former case, informers feared discrimination at the workplace or at school/university for themselves or their children. In the latter case people are reported to have felt "honoured" that they had been chosen to contribute to the cause of creating a socialist state:

"At first I felt a little bit strange, but then I was really happy. I was happy that someone was interested in me and that I could do something really important. And that it would be for the protection of socialism was of particular importance for me. That's when I wrote into my diary: 'Now I am really important" – or something like that. I was very happy about that."[76]

This not only goes to show how the establishment of formal systems which facilitate the practice of "informing" encourages individuals to participate in those systems, but also how they can be used to manipulate those individuals to protect values which they may not otherwise have prioritised over their own feelings of respect for others and peer loyalty.

---

[69] These figures were taken from Gellately, R. (1992) "The Gestapo and German Society: Enforcing Racial Policy 1933-1945", Oxford University Press, Oxford, p. 61

[70] Mallman, K.M. et al. (1993), p. 241, translation by the author

[71] Diewald-Kerkmann, G. (1997), p.154

[72] Cited after Sauerland, K. (2000), p. 17, translation by the author

[73] These figures have been taken from Koehler, J.O. (1999) "Stasi: The Untold Story of the East German Secret Police", Westview Press, Boulder CO, pp. 7-8

[74] The number of inofficial contributors has been continually revised downwards since the fall of the wall in 1989 from over 600000 to around 100000. These figures have been taken from an official studie carried out by Helmut Müller-Ensberg and published in his book "Inoffizielle Mitarbeiter des Ministeriums für Staatssicherheit" (1996), 3rd ed., Links Verlag, Berlin

[75] Funder, A. (2003) "Stasiland: Stories from behind the Wall", Granta Books, London, p. 74

[76] Maennel, A. (1998) "Auf sie war Verlaß. Frauen und Stasi", Espresso/Elef. Press, Berlin, p.45, translation by the author.

The psychological, social and political consequences of this impressive surveillance network as well as similar networks employed by other totalitarian regimes have been widely discussed. Like all comprehensive surveillance systems both the Gestapo and the Stasi networks tended to "undermine trust and, through [their] emphasis on individual behaviours, to undermine social solidarity as well"[77]. At the same time such systems augment "the power of those who institute [them] without increasing their accountability"[78]. People who live in an atmosphere where they do not know whether their every move is being watched and reported to the authorities will seek to conform to the rules of the ruling system. Rather than resist the oppressive forces many withdraw into what has been called "internal emigration". " They shelter […] their secret inner lives in an attempt to keep something of themselves from the authorities".[79]

The often disastrous effect of denunciation was officially recognised by the Allies after the end of the war, when a number of Gestapo informers were prosecuted for the commission of crimes against humanity under Control Council Law No. 10. In most of these cases the courts held that the offenders could not rely on the argument that they lacked an understanding that what they were doing was wrong, since their attitudes had violated commonly accepted moral laws[80].

Naturally, the establishment of whistleblowing systems in an employment context cannot be compared to surveillance systems set up by totalitarian regimes. However, Germany's historical experiences with denunciation go some way in explaining its reluctance to allow the establishment of formal reporting systems for the protection of often unspecified "common goods" which permit informers to use those systems anonymously and with limited accountability. In contrast to Anglo-American jurisdictions, there can be no unqualified acceptance of informing/whistleblowing as pro-social behaviour and laws which protect the whistleblower's interests over those of the person accused of wrongdoing. Instead, one might expect Germany to recognise a need for dual protection of both the whistleblower from retribution and the target of the allegation from untrue and unjustified accusations. It is therefore necessary to examine Germany's legal and constitutional framework within which whistleblowing schemes must operate in order to evaluate the unique situation companies employing such schemes find themself in.

5.2. Protection of the whistleblower

The extent to which a jurisdiction views whistleblowing as desirable, "lawful" behaviour can be measured by the extent to which it grants legal protection from retaliation to the whistleblower. In an employment context, this relates, in particular, to the extent to which the whistleblowing employee is pretected from unfair dismissal and other discriminatory measures by his employer. The act of whistleblowing, particularly where the recipient of the report is external to the organisation, can be seen as a breach of a contractual obligation of loyality[81] employees owe their employer, including, for example, an obligation to keep confidential any business internal information. The existence of such an obligation and its breach may justify the dismissal of the whistleblower under §626 of the German Civil Code (BGB) because of the employee's "behaviour"[82].

While it cannot be denied that the state and the public will often have an interest in the disclosure of information by the employee, for example where this relates to the violation by the employer of health and safety provisions or where the employer is alleged to have committed a criminal offence, the employer arguably has a vested interest in maintaining a climate of mutual trust between employees and between himself and his employees which might be affected if employees feel that they have the right or the obligation to spy on each other and, in this context, to disclose possibly business-sensitive information to a third party. Some commentators argue that employees' obligation of loyalty is in any case limited by their constitutional rights[83] as well as their legal rights[84] obligations obligations[85] to disclose certain information to the relevant authorities.

---

[77] Lyon, D. (2003) "Surveillance after September 11", Polity Press, Cambridge, p. 142

[78] id.

[79] See Funder, A. (2003), p. 96

[80] See, for example, Urteil vom 9.9.1947, in Justiz und Verbrechen, Vol. 1 (1968), pp. 663

[81] For an excellent description of the historical roots of such an obligation of loyalty in German law, see Müller, M. (2002), pp. 427-429

[82] "Verhaltensbedingte Kündigung"

[83] Müller lists the employees' freedom of opinion and freedom of speech (Article 5 I of the German Constitution (GG)), the right to participate in criminal prosecutions (Article 2 I GG in conjunction with Article 20 III GG) and the right to petition public authorities (Article 17 GG); Müller, M. (2002), p. 430.

5.2.1. German case law on whistle blowing

As already mentioned[86], only a few cases of whistleblowing have been decided by the German courts to date. They all deal with reports or the disclosure of information to business-external authorities and the decisions are unlikely to be directly transferable to business-internal whistleblowing scenarios.

However, closer inspection of those cases shows that the courts' willingness to protect the whistleblower from unfair dismissal is influenced not only by changing historical, political and social circumstances but also by questions of the legitimacy of the reported behaviour, employee motivation and whether or not it would have been necessary/more appropriate for the whistleblower to attempt to address the situation himself.

In the first decided case on whistleblowing in 1959, the Federal Employment Court (BAG) examined whether an employer was justified in dismissing an employee who had instituted criminal proceedings against him for violations of transport and hauling regulations[87]. Although the Court accepted not only that the employee's accusations were correct but also that the employee, by following his employer's instructions, was at risk of committing a criminal offence himself, it held that the employee's dismissal had been lawful, since the employer's claim to the employee's loyality outweighed all other considerations and the employee could have refused to carry out the employer's instructions where they would have required him to break the law. The tone of the decision betrays a strong “anti-informer” attitude of the court which may be explained by it proximity in time to the end of the NS-Regime. At a time when former NS-informers were still prosecuted for denunciations during the Third Reich, the court might have felt that a decision which would encourage further “denunciations” would be giving the wrong signal. Subsequent decisions[88] increasingly take into account the employee's motivation for reporting the employer's illegal behaviour as well as the question of whether the accusation was in fact correct. If the employee's report was an appropriate reaction to the employer's offence[89] and provided that the employee did not knowlingly or carelessly make false accusations against the employer[90], it was held that the accusation did not justify the employee's dismissal under §626 BGB[91]. At the same time, if an employee, because of the breakdown of a personal relationship with the employer, reported him to the revenue because of alleged tax evasion, she could not argue that she was justified in her actions because they might also benefit the common good of correct and fair revenue collection[92].

The progress towards more comprehensive rules of protection for the benefit of whistleblowers seems to have reached its provisional conclusion in 1996 when the employment court in Cologne had to decide a very similar case to that which was the subject of the 1959 BAG decision[93]. Ignoring the BAG’s arguments in favour of employee loyalty as the higher value, the court concluded that the dismissal of an em-

---

[84] Statutory rights of employees to report certain events or behaviour of others are rare and arise mainly in the area of environmental law. For example, employees have the right to report violations of certain environmental requirements relating to emissions, water quality and waste disposal to special environmental ombudsmen appointed by the employer under §§53 of the Federal Protection from Emissions Act (Bundes Immissions Schutz Gesetz - BImSchG), §§21a of the Water Protection Act (Wasser Haushalts Gesetz – WHG) and §§11a Waste Disposal Act (Abfallgesetz – AbfG)

[85] For instance, the obligation to report to the police plans for the commission of certain specified criminal offences under §138 of the German Criminal Code (StGB). Anyone failing to report such plans despite having “credible knowledge” of them, is liable to a fine or imprisonment of up to 5 years. See also BVerfG (2.7.2001) NZA 2001, 888 for a decision by the constitutional court which held that an employee which complies with his obligation as a citizen to appear as a witness in a criminal trial against his employer may not be dismissed by his employer because of this, even if the employer is acquitted of any offence.

[86] See note 61 supra.

[87] BAG (5.2.1959), Neue Juristische Wochenschrift 1961, 44. for a similar decision see also LAG Berlin (25.11.1960), Betriebs Berater 1961, 449

[88] For example,

[89] See for example Ascheid, R., Preis, U. and Schmidt, I. (2004) “ Kündigungsrecht - Großkommentar zum gesamten Recht der Beendigung von Arbeitsverhältnissen” (2nd ed.), C.H.Beck, München, §626, Nr. 190

[90] BAG (3.7.2003) AP KSchG §1, Nr. 45

[91] See for example Ascheid, R., Preis, U. and Schmidt, I. (2004) §626, Nr. 193. Some sources argue that the employee should still be required to exhaust internal means of bringing the violation to the attention of his superiors before filing a formal complaint

[92] BAG (4.7.1991) Rechtsprechung zum Kündigungsrecht (RzK) 6a I Nr. 74; see also LAG Köln (7.1.2002) NZA-RR 2002, 585

[93] see note 87 supra

ployee of a haulier business who had reported his employer for violations of traffic and vehicle safety regulations was void, since the employee had had reason to doubt the vehicles' roadworthyness and because his repeated attempts to resolve this issue directly with his employer had been ignored by the latter[94]. However, the court specifically left open the question if its decision would have been different, had the employee take additional steps against the employer or had he also informed the press or the public about the violations.

5.2.2. Dismissal after the introduction of a whistleblowing hotline

To date, there have been no cases where an employee has been dismissed following a report of illegal behaviour to an insider of the organisation whether in accordance with the organisation's line management structure or through an act of whistleblowing. It seems likely, however, that the courts would not permit employers to dismiss employees who have genuinely tried to act in the best interest of both the employer himself (for example, when reporting the illegal actions of a superior, of which the employer may not have been aware) and of their co-workers and/or the general public (for instance, in the case of health and safety violations). Of course, there is a danger that employers could try to "take revenge" on whistleblowers by dismissing them for charges other than the act of whistleblowing itself. Employee may then find themselves at a disadvantage when it comes to providing evidence for their contention that their decision to blow the whistle was the real reason for the termination of their contract.

Where the employer has introduced an ethics code of conduct backed up by a requirement on his employees to report any violation of that code through a whistleblowing hotline, it could be argued that the employer should not have the right to dismiss an employee who follows this procedure. As Wisskirchen, Körber and Bissels argue, the introduction of these requirements ultimately serves the protection of the employer's interests[95] and amends the employees' contractual obligations, including their loyalty obligations. It thereby significantly alters the substance of the contractual relationship between employer and employees. The dismissal of employees following their permitted and desired use of the whistleblowing hotline would contradict the doctrine of "venire contra factum proprium"[96]. At the same time it could be argued that this does not preclude an employee's dismissal, if they, in circumvention or avoidance of the internal whistleblowing procedures, reports the violation to an external authority. In this case the existing interpretation provided by the courts would continue to apply, possibly with the effect of discouraging employees from blowing the whistle.

5.3. Protection of the accused co-worker

In order to establish how the rights of the co-worker accused of wrongdoing are protected in German law one must examine employment and data protection law as well as the constitutionally guaranteed personality right of the individual (Article 2 I of the German Constitution (GG)).

5.3.1. Whistleblowing hotlines and the German data protection regime

The Data Protection Directive was implemented in Germany through the Federal Data Protection Act[97] (BSDG). While the German Act differs in structure from the Directive it provides a similar data protection framework.

Under §4 BDSG, the processing of personal data[98] is only lawful if it is permitted or required by law or regulation or if the data subject has consented to such processing.

If the employer, as is usually the case, operates the whistleblowing system by establishing a call-centre the collection and processing of employee personal data through this system is permitted under §28 BDSG provided it is for the purpose of complying with a contractual obligation. The employer's right to collect and process employee personal data for the purpose of compliance with an "ethics" code of conduct must therefore be an integral part of the employment contract between him and the employee. Where the contract is silent on this issue the processing may still be permitted, if it is necessary for the

---

[94] LAG Köln (23.2.1996) NZA-RR 1996, 330

[95] Wisskirchen, G., Körber, A. and Bissels, A (2006) "'Whistleblowing' and 'Ethikhotlines'" in Betriebs Berater Volume 28/29, p. 1571

[96] id.

[97] Bundesdatenschutzgesetz

[98] Defined in §3 I BDSG

purposes of the legitimate interests of the employer provided that that interest is not overridden by an interest of the employee that such data should not be collected or processed (§28 BDSG).[99] In view of the fact that the introduction of whistleblowing hotlines is a relatively recent occurrence in Germany, it has been argued that in the majority of cases, the purpose for which employee data is used in the context of the operation of such hotlines will normally exceed the purposes contained in standard employment agreements[100].

In addition, §4b(2) BDSG provides that personal data must only be transferred to recipients outside the EEA, if the data subject has no interest worthy of protection that such a transfer should not take place. It is generally accepted that the data subject will have such an interest if the data are transferred to a recipient in a country which does not afford the data an adequate level of protection[101]. In accordance with the regime developed in the Data Protection Directive, the data controller will either have to individually assess whether the recipient country affords an adequate level of protection[102] or will want to rely on a „community finding of adequacy" by the European Commission[103] or an agreement between the transferror and the transferee in the form of the standard model clauses approved by the European Commission[104]. In relation to transfers to US entities, German law recognises that companies which have signed to the US Safe Harbor scheme are deemed to afford an adequate level of protection[105].

As the regulatory framework in Germany is based on and must comply with the European data protection regime set out in the Data Protection Directive, it is likely that the establishment of a whistleblowing scheme in Germany will only be possible in compliance with applicable data protection rules, if the scheme does at least comply with the recommendations of the Article 29 Working Party[106]. When implementing such systems companies must therefore ensure that reports are not made anonymously (except in specific circumstances), and that the content of the report is limited to specific areas (such as financial or accounting irregularities) and people (e.g. managers operating in these areas)[107]. The collection of personal data for any additional purposes will usually require the explicit consent of the employees. Obtaining that consent is likely to be impracticable and will rarely be successful.

5.3.2. Employment law and the right to co-determination

According to §1 I of the German Works Council Constitution Act (Betriebsverfassungsgesetz – BVerfG) every person or company operating a business with five or more permanent employees must establish a works council the members of which are elected in direct and secret elections by the workforce (§§7-20 BVerfG). The works council is responsible for representing the interests of the employees in negotiations with the employer on questions of legal, social and economic importance for the employees.
§87 BVerfG specifies a number of areas in which the works council enjoys a "right of co-determination". This means that in relation to measures which fall within the realm of those areas the works council has to be consulted, and in some cases must give its consent, before such measures can be implemented. This includes measures concerning:

- questions of internal company organisation and rules regulating the behaviour of the employees (§87 I No. 1 BVerfG);
- the introduction and application of technical arrangements which are designed to supervise or measure the behaviour or performance of employees (§87 I No. 6 BVerfG); and
- selection guidelines designed to assist any decisions about individual measures relating to human resources, where in the context of those decisions more than one employee or applicant may be suitable (§95 BVerfG).

---

[99] Article 7(f) of the Data Protection Directive
[100] See, for example, Wisskirchen, G., Körber, A. and Bissels, A (2006), p. 1567
[101] Gola, P. and Schomerus, R., Kommentar zum Bundesdatenschutzgesetz, (2005), 8th ed.,C.H. Beck, Munich, §4b, paragraph 3.2
[102] id., paragraph 4
[103] id., paragraph 5
[104] id., paragraph 5.3. See also note 60 supra.
[105] id., paragraph 5.2
[106] See paragraph 4.2.
[107] Wisskirchen, G. et al. (2006), p. 1570

The question of whether the introduction of US-style “ethics codes”, which in many cases regulate in some detail the behaviour expected of an organisation's employees, aree subject to the works council's right to co-determination was resolved in a case brought by the works council of a German subsidiary of US-company Wal-Mart in 2005. The case was originally heard by the employment court in Wuppertal[108] whose decision was later appealed by Wal-Mart to the employment appeal court in Düsseldorf[109].

Following, among other things, the coming into force of SOX in the US, Wal-Mart had adopted an ethics code of conduct which regulated not only questions of financial and accounting propriety but also included:

- a prohibition to accept gifts and inducements;
- rules governing harassment and inappropriate behaviour;
- rules governing rights of access to personnel files;
- a prohibition of romantic relationships between co-workers if one of them is in a position to influence the working conditions of the other; and
- a requirement that a drugs test would be carried out as part of the recruitment process. 110

Wal-Mart’s works council had argued that such wide-ranging regulation of employee behaviour could not be introduced without its prior consultation.

The appeal court concluded that:

- an obligation imposed on employees by an employer to report any violation of an ethics code to their line manager or to an “ethics office” via an anonymous telephone hotline was subject to the work council's right to co-determination under §87 I No. 1 BVerfG.
- where the ethics code provided that employees must not accept any gifts or inducements from suppliers, the works council had a right to co-dermination under §87 I No. 1 BVerfG with regard to the question if this prohibition also applied to objects of daily use such as biros, diaries, cigarette lighters etc. and how employees should behave in this respect.
- where the ethics code prohibited the harassment of co-workers without limiting this prohibition to sexual harrassment, the works council had a limited right of co-determination111.

The appeal court made it clear that it expected the Wal-Mart works council to agree to the majority of the regulations contained in the ethics code as they were mostly reasonable and clearly served the protection of the employees it represented. At the same time, by establishing that such regulations could only be introduced following proper consultation of the works council, the decision not only defended the works council's rights under §§87 and 95 BVerfG, but also established the limits to the extend to which employers may prescribe the behaviour of their employees.

5.3.3. The “personality right” protected in Article 2 I GG

In relation to the prohibition on romantic relationships between co-workers, the lower court in Wuppertal had held that this, too, was subject to the work council's right to co-determination. However, this argument was rejected by the appeal court which concluded that, rather than beingsubject to such a right under the BVerfG, an ethics code which included such a prohibition violated the individual rights set out in Articles 1 and 2 GG. It was therefore null and void.

The appeals court argued that those provisions defined human dignity and an individual's personality right as central values of the German constitution which had to be observed by everyone as long as the exercise of those rights did not violate the rights and freedoms of others or breached constitutional or moral

---

[108] Arbeitsgericht Wuppertal in its decision of 15.6.2005, 5 BV 20/05, NZA-RR 2005, 476
[109] See Urteil d. LAG Düsseldorf vom 14.11.2005, 10 TaBV 46/05, BB 2006, 335 = NZA-RR 2006, 81.
[110] LAG Düsseldorf, see note 109
[111] id.

principles. The personality right included the right of each individual freely to decide if and with whom it wished to enter into a relationship, whether as friends or lovers.

The court found that the life of employees was influenced and determined to a significant extend through their employment relationship. Employees' human dignity was not only affected by the question of if and how they performed their duties but also by the question whether or not and with which co-worker they could maintain friendships and romantic relationships. Where they were prevented from entering into a personal relationship with a co-worker or superior even in the private sphere, employees had to assume that theirs was only to work and that they had to "hand in their personality rights at the company reception"[112].

Although the appeal court's decision mainly concerned the question of whether the Wal-Mart ethics code was compliant with German legal and constitutional guarantees, one could argue that it indirectly affects the question of whistleblowing at least where an enforceable requirement to report a violation of that code exists. Such a requirement to report an "offence" cannot be lawful where the "offence" itself has no legal basis or authority. Nonetheless, where ethics codes remain unchallenged, employees may well feel that it is in their best interest to comply with their requirements. For this reason, it is submitted that the court was right to emphasise the works council's right to co-determination as this concept at least provides a certain control mechanism which, in the medium term will serve to restrain employers from including in their ethics codes "soft law" rules which directly affect the rights and freedoms of their employees without directly being subject to the rule of law and judicial review.

6. Conclusion

In its refusal to allow ethics hotlines in the cases of MacDonalds and Excide, the French CNIL held that to do so would „re-enforce the risk of slanderous denunciation" and the stigmatization of employees who were the subjects of an ‚ethics alert'"[113]. On the other hand, advocates of the practice argue that a failure to provide legal protection from retribution to whistleblowers will result in a situation where employees are acticely discouraged from bringing unfair and unlawful behaviour to the attention of the employer or the appropropriate authorities, thereby preventing them from remedying the situation and from adequately protecting accepted public and private interests.

In view of Germany's recent experience with denunciation and Stasi-informers it is unsurprising that German courts, in particular, seem to feel deeply uneasy not only about permitting the use of reporting procedures in circumvention of established line management and authority structures but also about the introduction of new "soft law" rules adopted by private companies rather than elected governments without due regard to individual rights and the rule of law. Not only will those companies normally be in a position of power in relation to the rules' addressees but they may also have their own subjective political, moral or religious agenda which they would not otherwise be permitted to impose on their employees.

As Jubb argues, there is a risk of confusion between a whistleblower and an informer.

"That broad assumption which juxtaposes the whistleblower with, say the corrupt individual turned informer is quite undesirable, not because whistleblowing is above reproach but because it is severely tainted already."[114]

In order to avoid the risk that whistleblowing will become interchangable with, and not recognised as a special case of, "informing"[115], a more restrictive definition of whistleblowing is therefore necessary, one which takes into account the rights and interests of the whistleblower, the person accused of wrongdoing and society as a whole. There is a balance to be struck between defending social and democratic principles and the risk of "overdefending" or seeking to defend the "wrong" or merely subjective principles.

Provisions protecting the whistleblower from retaliation, for example by allowing him or her to make reports anonymously and in circumvention of established line management structures, are only appropriate if two conditions are met:

---

[112] id., translation by the author.
[113] Note 3 supra.
[114] Jubb, P.B. (1999), p. 77
[115] id.

1. The standard or value the whistleblower intends to protect must bee based on strictly defined legal requirements designed to protect specified, democratically adopted and constitutionally guaranteed public interests or individual rights and freedoms, to the exclusion of subjective moral value judgements. Companies, in particular, should not be free to include into ethics codes they are required to adopt for one purpose (in the case of SOX the protection of commonly accepted finance and accounting standards) additional behavioural requirements which affect their employees' privacy and personality rights.

2. The organisational structures facilitating the act of whistleblowing must be designed to prevent whistleblowers from engaging in behaviour which is largely motivated not by altruistic but by selfish motives and which may leave the person accused of wrongdong without legal protection. While it is true that whistleblower may have self-serving as well as altruistic motives for their complaint, a balance must be struck to ensure that the procedure is not abused by them for their own selfish purposes. The requirements of section 301(4) SOX should be tightened in accordance with the EC Working Party's recommendations. This could be achieved by restricting the number of individuals permitted to use the procedure as well as the number of individuals about whom complaints may be made. Whistleblowers should only be granted anonymity in exceptional circumstances and in any case only until the employer has examined the complaint. If he decides to take steps against the person accused of wrongdoing on the grounds that the complaint was justified, that person should be given all the information necessary to enable him or her to defend themselves against the accusation. This would include the identity of the whistleblower, except in very rare cases, for example where the whistleblower is expected to continue to work under the control of the accused person on a day-to-day basis. If the employer finds that the accusation was unjustified, the measures taken against the whistleblower should depend on their motivation for making the complaint. Where they acted in bad faith, the person accused of wrongdoing should be informed of the whistleblower's identity so as to be able to take steps against them. Where the complaint was due to a genuine mistake, the employer may choose to preserve the whistleblower's anonymity in order to maintain a work climate of mutual trust.

At the same time, it is necessary for German law to provide better protection for genuine whistleblowers from retribution and discrimination by their employers. The idea that an employer should have the right to unquestioning loyalty from his employees, which still seems to underlie many of the judicial decisions in this area, is outdated and outmoded in view of the changed reality of employer-employee relationships[116]. Where employers are indeed found to be in breach of their contractual or statutory obligations, it is not the employer but the whistleblower who deserves protection.

As Brinker Dozier and Miceli put it:

„[...], if the act of whistle-blowing involves only potentially positive outcomes to others and little expected cost or benefit to the observer and is likely to be followed only by outcomes deemed ‚good' by society[117], it can be considered altruistic"[118].

On the other hand, one must not loose sight of the fact that some (political and commercial) systems strive for the adoption of their subjective values by the majority. Those systems will make every effort to get to a situation where everything can be seen and heard and where the private sphere is reduced to a minimum. When used without restrictions or oversight, whistleblowing procedures can therefore turn into an extension of an organisation's panoptic gaze which enforces values which may not otherwise be enforceable and which involves the surveilled in the process of their own surveillance at the expense of peer loyalty, social trust and solidarity.

---

[116] See Müller, M. (2002), p. 428

[117] Within a democratic and constitutional framework.

[118] Brinker Dozier, J. and Micel, M.P. (1985), p. 825