# Compliance in Unprecedented Times

CEJ
COMPLIANCE ELLIANCE JOURNAL



Content Curators:
Michele DeStefano (University of Miami School of Law)
Dr. Hendrik Schneider (University of Leipzig Faculty of Law)

ISSN 2365-3353
Volume 6 • Number 1
Spring 2020

Compliance Elliance Journal (CEJ)
Volume 6, Number 1, 2020
ISSN: 2365-3353
This version appears in print and online. CEJ is published twice per year, in spring and fall.

Title: Compliance in Unprecedented Times

Content Curators:
Michele DeStefano, University of Miami School of Law and LawWithoutWalls
Dr. Hendrik Schneider, University of Leipzig Faculty of Law

Technical Support:
Hannah Beusch
Hans-Henning Gonska
Dr. Niels Kaltenhäuser
Jannika Thomas

Website: www.cej-online.com

Email: info@cej-online.com

Address:
Taunusstrasse 7
65183 Wiesbaden, Germany

Telephone: +49 0341 / 97 35 220

Copyright © 2020 by CEJ. All rights reserved. Requests to reproduce should be directed to the content curators at info@cej-online.com.

CEJ
COMPLIANCE
ELLIANCE
JOURNAL

# Compliance in Unprecedented Times

## TABLE OF CONTENTS

CEJ
COMPLIANCE
ELLIANCE
JOURNAL

# EDITORIAL

## COMPLIANCE IN UNPRECEDENTED TIMES

Our daily life has experienced significant upheavals and cuts within the last months. Whereas the sufferers and their relatives are hit the hardest by the covid-19 pandemic, the protective measures turn our economies upside down. Thus, digital applications and remote-solutions experience a shock-implementation. Now it shows how essential the innovative strength in the digital sector is for all of us. The topics of e-health and digital teaching, which have been focused on in previous issues of the journal, are coming now into effect – with an unforeseeable urgency.

Therefore this edition of CEJ is dedicated to pressing criminal and compliance-related questions in connection with the coronavirus-pandemic. Furthermore we will focus on another branch of digitization: Namely cryptocurrencies and financial technology. The key issue of last CEJ-edition, Corporate Criminal Liability, will be deepened, as there have been notable (and given the current situation, questionable) developments in the German legislative process. Fittingly, the topic of whistleblower protection in Switzerland will be addressed and two books, dealing with the modern legal advice market, will be reviewed.

We aim to continue the debates initiated by this issue and are interested in articles from all over the world. We eagerly await your respective impulses and hope you enjoy the lecture of this special issue!

With our best regards,

**Michele DeStefano & Hendrik Schneider**
Founder and Content Curators of CEJ

CEJ
COMPLIANCE
ELLIANCE
JOURNAL

# BETWEEN CRIMINAL LAW AND CORPORATE SOCIAL RESPONSIBILITY - DRUG DONATIONS TO HCPS AND HCIS IN THE AGE OF THE CORONAVIRUS

Kai C. Bleicken, Elisabeth Engels & Hendrik Schneider

## AUTHORS

*Attorney Kai Christian Bleicken, Managing Director of AKG e.V., Berlin.*

*Attorney Elisabeth Engels, AKG e.V., Berlin.*

*Prof. Hendrik Schneider, Chairman of the AKG e.V. Expert Committee "Healthcare Compliance Advisory Board", proprietor of the office Gutachten&Strafverteidigung, Wiesbaden.*

*AKG e.V. stands for Arzneimittel und Kooperation im Gesundheitswesen e.V. (Association for Drugs and Cooperation in Healthcare). The AKG was founded in November 2007 and is the organization with the largest number of members in the area of voluntary self-regulation of the pharmaceutical industry in Germany. The AKG gives top priority to compliance with codified rules on competition and conduct according to the practice-based principle of "prevention before sanction". As a body involved in self-regulation of the pharmaceutical industry, the AKG supports its members in ensuring transparent and fair corporate conduct in the cooperation between the pharmaceutical industry and the medical profession. The AKG has a Code of Conduct which contains regulations for the cooperation of member companies with doctors, hospitals and other health care institutions and which is binding for member companies*

Federal Finance Minister Olaf Scholz wants to give tax concessions to companies that donate disinfectants, protective masks and other medical goods during the coronavirus crisis. The minister was quoted by the news agency Reuters on April 3, 2020 as follows: "Many donations are being made to hospitals, medical practices and nursing homes. This should be encouraged. Medical donations in kind are now exempt from VAT." Such donations are not only politically desirable, but also an expression of corporate social responsibility, i.e. the voluntary contribution of a company to overcoming the current social and economic problems and a way of assuming a corresponding share of responsibility. However, these good intentions alone do not override the compliance rules and limits of criminal law on permissible benefits to healthcare professionals (HCPs) and healthcare institutions (HCIs). Under German criminal law on corruption, such donations constitute "benefits" or "third-party benefits", which can fall under §§ 299, 299a, 299b, 331 ff. of the German Criminal Code. The following limits must be observed:

**1.** The AKG Code of Conduct covers donations, which include monetary donations and the donations in kind concerned here, in § 22. § 22 (1), (3) AKG Code of Conduct limits the permissible recipients of donations in accordance with tax law (§ 10b of the German Income Tax Act (EStG) and § 9 of the German Corporation Tax Act (KStG)). Accordingly, donations may not be made to individuals belonging to professional groups (§ 22 (3) AKG Code of Conduct), but only to institutions, organizations or associations of members of professional groups. In this context, the Code mentions hospitals, university clinics and medical-scientific professional associations as examples, which as a rule fall under § 10b (1) sentence 2 no. 1 EStG, § 9 (1) sentence 2 letter a KStG (legal entity under public law, e.g. university clinic operated in the legal form of an AöR) or under § 10b (1) sentence 2 no. 2 EStG, § 9 (1) sentence 2 letter b KStG, in each case in conjunction with § 5 (1) no. 9 KStG. Further conditions include the fact that the donation is made voluntarily and free of charge in order to promote tax benefits that help others. In this context it is not the internal motives that matter, but the external circumstances. A donation may therefore still have marketing objectives, for example, in addition to charitable and altruistic purposes. In connection with the principles of separation and documentation, § 22 (1) AKG Code of Conduct contains the restriction that "on objective assessment of the circumstances under which they are made, donations cannot be understood as influencing therapeutic, regulation or procurement decisions and shall be properly documented for a period of at least five years after they have been made". If drug donations are related to the additional demand caused by the crisis, this suggests that there is no possible intention to exercise such influence. Insofar as donations are made to HCIs and not to individual HCPs under the above conditions, drug donations are in compliance with the Code and will not be subject to criminal prosecution. Unless there is evidence to the contrary which suggests that there is an intention to influence decisions regarding procurement or regulations, the prerequisites of an unjust agreement that would constitute a criminal offense as described above are not met.

Medical device manufacturers are taking a somewhat different approach on the basis of the MedTech Europe Code of Ethical Business Practice of December 2015, section IV of which stipulates that grants to hospitals are generally not permitted. However, in connec-

tion with the coronavirus crisis, the committee has allowed member companies to support hospitals to overcome the crisis under certain conditions (see "Donation and Free of charge loans") by means of an additional internal guideline (MedTech Europe Code Committee Guidance, March 27, 2020). Donations can be made in the form of funds, capital goods, products, consumables, services or software (see "Types of emergency support/requests"). The donation should be related to immediate needs in connection with and for the duration of the coronavirus crisis (see "Donation and Free of charge loans").

**3.** On the other hand, donations are not permissible if the drugs are given to individual doctors or other HCPs. According to the AKG Code of Conduct, such donations are excluded. They fall under the prohibition of individual donations according to § 22 (3) AKG Code of Conduct and do not constitute permissible gifts according to § 21 AKG Code of Conduct. Firstly, the benefit is not granted for a reason that is explicitly covered by § 21 (2) AKG Code of Conduct. Secondly, the prohibition of individual donations in § 22 (3) AKG Code of Conduct may not be circumvented by a broad interpretation of § 21 (2) AKG Code of Conduct (see also the interpretation principle in § 4 (1) AKG Code of Conduct); and thirdly, in the case of donations to individual doctors, the recipient does not enjoy non-profit status, which is a prerequisite for a donation as defined under tax law and according to § 22 AKG Code of Conduct (more detailed information: AKG (ed.), At a glance, 3rd edition 2018, keyword "donation"). Finally, it should be noted that doctors do not dispense or use medicines, but only prescribe them. Except in certain exceptional cases, dispensing by doctors is precluded by the prohibition in § 43 (1) of the German Drugs Act (AMG) and § 17 (1a) of the German Pharmacy Operation Ordinance (ApBetrO). If it becomes apparent that these limits have been exceeded, the objectives pursued by the provision of the medicinal products to individual doctors may be examined. This can at least result in the risk of investigation for an offence involving corruption. Of course, this is not the case if no drugs are donated, but disinfectants, breathing masks or protective clothing, which doctors and dentists in practices urgently need.

**4.** Finally, the prohibition on benefits under § 7 (1) of the German Advertising of Medications Act (HWG), which also applies to HCIs pursuant to § 2 HWG, must be observed. In the above case of donation of, for example, disinfectants or respiratory masks, there is no cause for concern that § 7 (1) HWG may have been infringed, because the donations are not considered to be product-related sales advertising for a specific medication within the meaning of § 1 (1) no. 1 (unless the products in question are printed with a drug name, for example). Accordingly, the HWG does not apply. The situation may be different if the drug donation is used to advertise the use of the drug in therapy. In this case, the advertising material is identical to the advertised product. This entails the risk that the donation may be unlawful pursuant to § 7 (1) HWG. A violation of § 7 (1) HWG constitutes an administrative offense pursuant to § 7 (1) no. 4 HWG. Since § 7 (1) HWG is a market conduct standard, infringement of that provision also suggests the existence of an agreement which is unlawful under §§ 299, 299a, 299b and 331 et seq. of the German Criminal Code.

**5.** Caution is also required if the donation of a drug is accompanied by an implied invitation to off-label use. At present, various active ingredients are being used which are said

to be effective against coronavirus or at least have a function that supports the recovery process. If this relates to products that are used or are intended to be used outside of approval, the advertising ban of § 3a sentence 2 HWG applies, which is also covered by § 9 sentence 2 AKG Code of Conduct. If it is possible to interpret the donation as advertisement of off-label use, this can also be regarded as an intention to influence the donor and may entail the corresponding risks of prosecution under criminal law for an offence of corruption.

In summary, donations of medications should therefore only be made to hospitals or their pharmacies and not to individual medical bodies or individual doctors. Professional medical bodies may be institutions that enjoy tax benefits and are in principle legitimate recipients of donations in kind. However, professional bodies do not treat patients, with the result that the legitimate purpose of the drugs is questionable and would have to be defined more precisely in the context of earmarking the donation. There is no risk of conflict with the law if the benefits cannot also be regarded as product-related sales advertising and do not entail an invitation to off-label use.

CEJ
COMPLIANCE
ELLIANCE
JOURNAL

# LIABILITY FOR ENTREPRENEURIAL RISK DECISIONS DURING THE COVID-19 CRISIS

Michael Kubiciel

## AUTHOR

*Michael Kubiciel is a professor of criminal law at the University of Augsburg / Germany and leads a research group for corporate criminal law based there.*

## ABSTRACT

*The article deals with the liability of board members for decisions to minimize business risks resulting from the pandemic. Based on an important decision by the highest German criminal court on a case of the 2008 financial crisis, the article outlines the limits of a safe haven within which managers can make decisions without fear of legal consequences.*

The rapidly spreading pandemic is putting companies under considerable pressure. Boards of directors and managing directors have to make far-reaching decisions in the shortest possible time with considerable uncertainty in forecasts. It is clear that not every decision will have the desired success; some will perhaps cause more harm than good.

This also raises the question of civil or even criminal liability risks. A decision made by the BGH (German Federal Court of Justice) from 2016 is of considerable importance to answering this question. It was based on facts that show structural parallels to the current situation. This refers to the decision on the criminal liability for breach of trust of those responsible at HSH Nordbank who, under great time pressure during the financial crisis of 2007, carried out a transaction to relieve the burden of debt, but who – as became apparent later – thus caused the bank to incur a loss of just under EUR 150 million[1].

The responsible persons at HSH Nordbank – like many members of the management board in the current crisis – had to make an atypical risk decision. The object of its activities is not the ordinary course of business, which entails risks as well as new opportunities. Rather, measures are required to reduce risks arising from a sudden change in the business environment, the dynamics of which are hardly foreseeable. Mitigating these risks may require measures that would have been unthinkable just a few days ago – from abandoning a transaction to postponing urgently needed investments, temporarily closing plants or applying for government deposits.

When it comes to crisis management, board members and managing directors operate in front of an open horizon, just like politics: Only the future will tell whether the drastic measures are ultimately necessary and successful – but action must be taken now. In contrast to politics, however, managers and entrepreneurs bear a considerable personal liability risk. If they act wrongly, they not only risk loss of reputation and, in the worst case, of office, but also substantial legal consequences.

As a result, those responsible in companies find themselves in a dilemma situation in which both options for action – immediate action and further waiting – are risky and in which every decision made may prove to be wrong in retrospect. It would therefore be highly unfair to make the occurrence of legal consequences dependent on the outcome of the decision. In addition, a "negative success liability" would have harmful effects on companies and the economy, as it would lead to a slowing down and distortion of decision-making processes: Managers may be inclined to act only at a time when an option has

1 BGH, NJW 2017, 578 with comments from Alexander Baur & Maximilian Holle, *Untreue und unternehmerische Entscheidung*, ZEITSCHRIFT FÜR WIRTSCHAFTSRECHT, 555 (2017); Michael Kubiciel, *Anmerkung*, JURISTISCHEZEITUNG, 72, 585 (2017); Alaor Leite, Prozeduralisierung oder Rechtsgüterschutz bei der Untreue? - Risikoverringerung in der Unternehmenskrise am Beispiel der HSH-Nordbank-Entscheidung (BGH NJW 2017, 578), 580 (2018); Ulrich Leimstoll, *Erfordernis einer gravierenden Pflichtverletzung beim Untreuetatbestand (»HSH Nordbank«)*, STRAFVERTEIDIGER, 388 (394) (2017).

expired or has proven to be clearly incorrect. Valuable time to reduce risks for the company would then be lost.

In order to prevent this, case law (with different approaches that are not always consistent) is trying to limit liability risks. In its HSH Nordbank decision, the 5th Criminal Division of the BGH (German Federal Court of Justice) clarified that a violation of (stock corporation law) due diligence obligations is only present in the case of "absolutely unjustifiable" conduct[2].

It is important to know that the Criminal Division does not interpret § 266 StGB (German Penal Code) here, but rather interprets § 93 para. 1 AktG (German Stock Companies Act), to which the accessory offence of breach of trust refers. The remarks of the Criminal Division on the clarification of the scale of obligations are therefore just as relevant for the application of company and liability law as for § 266 StGB.

According to the opinion of the 5th Criminal Division, an "unjustifiable action" is only present if the mistake has already forced itself upon an outsider. What sounds like a very wide scale, however, becomes considerably narrower when one reads the further remarks of the Division. Such an error could also consist in the inadequate collection and analysis of information prior to a decision.

However, case law also accommodates decision-makers in a crisis situation. It is necessary, but also sufficient, for the board of management to obtain an "appropriate" factual basis, taking into account the time factor and weighing up the costs and benefits of further information acquisition. It is not important that the decision was actually taken on the basis of adequate information and in the best interest of the company. Rather, it should suffice that the board of management was "reasonably" allowed to assume this at the time of the decision.

These – admittedly soft – criteria provide the decision-makers in the companies with what they now need most urgently: a sufficiently large "safe haven" for decisions.

2 for this criterion, see Michael Kubiciel, *Gesellschaftsrechtliche Pflichtwidrigkeit und Untreuestrafbarkeit*, NEUE ZEITSCHRIFT FÜR STRAFRECHT, 353 (2005).

CEJ
COMPLIANCE
ELLIANCE
JOURNAL

# NON-PAYMENT OF RENT DUE TO THE CORONA PANDEMIC - LEGALLY AND ETHICALLY JUSTIFIABLE?

Tim Drygala

## AUTHOR

*Prof. Dr. Tim Drygala holds the Chair for Civil Law, Commercial and Company Law at the University of Leipzig.*

## ABSTRACT

*The announcement by Adidas, Deichmann and H&M to stop paying rent for their closed shops beginning in April has caused quite a stir. Tim Drygala explains why such behavior is covered by case law.*

## TABLE OF CONTENTS

On March 25, 2020, the German legislator adopted the Law on the Mitigation of the Consequences of the Corona Pandemic in Civil, Insolvency and Criminal Proceedings.[1] The law temporarily forbids the contractual termination of tenancies. If the tenant defaults on a rent payment, the lessor's normal right of termination is suspended until the end of June, provided that the loss of payment is demonstrably due to the Corona pandemic. The tenant is given until mid 2022 to pay off the debt.

Right after the announcement of the law, several large retail chains stated that they would not pay their rent for April 2020 due to the closure of the shops as ordered by the government, although liquid funds would be available for this purpose. This led to heated discussions; in public, this type of behavior has often been seen as lacking solidarity. The Federal Minister of Justice announced that it would be indecent and unacceptable if financially strong companies simply stopped paying their rent. Only if tenants actually ran into serious difficulties paying rent as a result of the crisis could those tenancies not be terminated for a limited period of time.

But is this true? Political assessments need not necessarily be legally sound. Perhaps it is only the sense of justice that sees the lessor here as the party in need of protection and the tenant in the obligation to pay as long as the tenant is not threatened with insolvency. The Austrian General Civil Code (ABGB), which came into force as early as 1812, explicitly addresses the problem of epidemics in tenancy law. Art. 1104, which remains unchanged to this day, states: "If, due to extraordinary circumstances, such as fire, war or epidemic, [...] the object intended to be held cannot be used or put to use at all, the owner of said object is not obliged to restore it, but no rent or lease payment is due."

## I. IMPOSSIBILITY OF CONTRACTUAL USE

The Austrian Civil Code (ABGB) does not refer to any risk of insolvency and/or an internal connection between the obligation to pay and the epidemic; however, the simple impossibility of contractual use is sufficient. And on a sobering note, there is also much to be said for this regulation. After all, why should the tenant continue to pay, even though the tenant gets nothing useful in return? And is it not the case in principle that in tenancy law, unlike the law on contracts for the sale of goods or for work and services, the risk of accidental deterioration does not pass to the tenant but to the lessor, as the lessor remains responsible for the fitness for use of the rented property regardless of fault?

Since this is the case, German case law has extended the concept of defects in Section 536 of the German Civil Code (BGB) despite the lack of a statutory provision. The defect can also be recognized as consisting of an external effect on the rental object if this directly affects its practical value. This is (aptly) called an 'environmental deficiency'.

---

1 Annelie Kaufmann & Tanja Podolski, *Das steht im Corona-Maßnahmenpaket*, LTO, (Apr. 13, 2020) https://www.lto.de/recht/hintergruende/h/corona-bundesregierung-gesetz-infektionsschutz-strafverfahren-krankenhaus-solo-selbststaendige/.

Recognized examples include construction measures in an adjoining building that force closure of the other building (Federal Court of Justice (BGH), judgement dated April 23, 2008, Case No. XII ZR 62/06) or the blocking of an access area (District Court of Berlin (KG Berlin), judgement dated November 12, 2007, Case No. 8 U 194/06). Indirect impairments, in particular unexpectedly weak customer traffic in shopping malls (Federal Court of Justice (BGH), judgement dated February 16, 2000, Case No. XII ZR 279/97), are irrelevant. In the case of measures ordered by governmental authorities, it is necessary that the measures are directed against the operation and not against the tenant itself (Federal Court of Justice (BGH), judgement dated July 13, 2011, Case No. XII ZR 189/09). All this is fully[2] recognized by the courts, and the discussion is now mainly focused on whether this legal consequence can be limited or waived in the lessor's contractual terms and conditions.

On the basis of this case law, commercial tenants may rightly refuse to pay. This is because the usability has been rendered impossible, as the state has directly intervened against the operation of the business but not against the operator itself. It would be too subtle to argue that the business itself is not prohibited from operating, only customers have been prohibited from entering the business. After all, the shop is rented out as a retail store, so that usability as storage space or for a delivery service is not an argument. And a change of use would also be completely uneconomical, considering the associated rebuilding requirements. More serious is the objection that the current closures do not relate to the leased property but to the business purpose pursued. In particular, grocery stores and bank branches are open regardless of their location, whereas textile and shoe shops are closed regardless of their location, although in the cases decided so far it was precisely the unfavourable location of the shop (next to a construction site, on a closed road, etc.) that led to an 'environmental deficiency' being assumed.

However, it could be countered that this would increase the problem for the tenant, as the tenant cannot escape the current invidious situation by giving notice and changing location. "The 'environment' in the sense of 'environmental deficiency' case law would therefore currently be the entire area affected by the closure. For the time being, we can only wait to see how the case law positions itself in these matters. Nonetheless, the suspension of payment by tenants is not arbitrary or unjustifiable. The case law certainly tends towards the solution of the Austrian Civil Code - no business, no money.

## II. PANDEMIC-RELATED RIGHT TO REFUSE PERFORMANCE?

The legislature is, of course, free to regulate the matter differently. And after all, according to the public statements made by the Minister of Justice on television and several members of parliament on Twitter and Facebook, he believes he has already done just that.

---

[2] Michael Selk, *Minderung der Gewerbemiete bei behördlich angeordneter Schließung?,* BECK-COMMUNITY (Apr. 13, 2020) https://community.beck.de/2020/03/27/minderung-der-gewerbemiete-bei-behoerdlich-angeordneter-schliessung?fbclid=IwAR160UBCDb4IYMirZiZ6AAOidK80LJ_wIdDrg-vFkFoQcTYGeAkOiVlrj3pg.

This leads to the crucial question: Is the Corona Mitigation Act possibly lex specialis to both Paragraph 536 of the German Civil Code (BGB) and the related case law? Does the law in fact contain no protection for the commercial tenant who could otherwise rely on Paragraph 536 of the German Civil Code (BGB)? Is the tenant therefore actually worse off?
The wording clearly argues against this. The regulation concerning the right to refuse performance in the new Art. 240 of the Introductory Act to the German Civil Code (EGBGB) Section 1[3] expressly does not apply to tenancy law, see there Section 1 Para. 4 No. 1. Furthermore, in the tenancy law regulation on the restriction of termination under Section 2 Para. 1, reference is made to "rent due", and rent that is reduced to zero is not due. However, the preamble to the law is all the more clearly based on the assumption that there is in itself an obligation to continue paying the rent. This is because it expressly states with regard to the restriction on termination: "The obligation of the tenants to pay rent fundamentally remains in place." Furthermore, the law generally shows a desire to support only those who are in economic distress as a result of the pandemic. Art. 240 Section 1 and Section 2 of the Introductory Act to the German Civil Code (EGBGB) both clearly indicate this.

The following is apparently what happened: The Ministry of Justice overlooked Section 536 of the German Civil Code (BGB) and the relevant case law when preparing the draft, and perhaps had residential rent in mind, whereby rooms remain usable. The haste with which the Corona Mitigation Act was passed may have contributed to this. The Ministry of Justice and the Bundestag tacitly assumed that a general right to refuse performance due to a pandemic does not exist and is not wanted by the legislature.
Rather, the law aims to maintain the flow of services as far as possible and to help only those who need help due to the economic situation. The intent of the legislature becomes apparent in that the restriction on termination in tenancy law should remain the only remedy. Therefore, it seems justifiable to put the slightly unfortunate wording behind us as an editorial error due to the haste of the legislative procedure and to help the unspoken intent of the legislature to come forth: A general pandemic-related right to refuse performance is unintentional because it only passes on the liquidity problems to the next person in the performance chain. For the time being, the case law on 'environmental deficiency' also takes a back seat to this. An explicit clarification by the legislature would be helpful, but not absolutely necessary in view of the intent expressed in the Corona Mitigation Act. The obligation to pay remains in force even in times of an epidemic.

## III. NEGATIVE PUBLIC REACTION AND BACKTRACKING BY ADIDAS

The strongly hostile reaction of politicians and the public has led Adidas to rethink its position. While at first it was said that the company would only freeze payments to commercial lessors, but would continue making payments to private lessors, on April 1, 2020,

3 Deutscher Bundestag, Entwurf eines Gesetzes zur Abmilderung der Folgen der COVID-19-Pandemie im Zivil-, Insolvenz- und Strafverfahrensrecht (Apr. 13, 2020), http://dip21.bundestag.de/dip21/btd/19/181/1918110.pdf

it was declared that rental payments would be made to all lessors. The realization has now prevailed that a payment freeze could possibly be even more damaging for the company than paying the rent for April 2020. Ultimately, however, the fear of negative customer reactions in the time after the shops reopen and of a loss of image was simply too great for Adidas - regardless of all legal arguments. Other companies that are less well known to the public, such as the shoe chain *Deichmann*, on the other hand, as far as can be seen so far, are sticking to the course they have taken. This is regrettable because the change of course by Adidas is not only in accordance with the intent of the legislature, but also makes economic and moral sense. As individually understandable as it may be to first protect one's own liquidity in an imminent deflationary crisis, this behavior is just as damaging at the macroeconomic level. This is because, with the cessation of rental payments, the economic difficulty shifts to the owner of the property, who must continue to bear operating and financing costs without having any income. If the latter, in turn, is having difficulties making payments, the problem will, in case of doubt, hit the bank that financed the property, and at this point at the latest, as seen in the crisis of 2008, the state will have to step in. A general pandemic payment freeze is therefore a typical policy of the beggar-thy-neighbor: Conserving one's own liquidity reserves is done at the expense of others and therefore ultimately of the general public. It is therefore the right policy of the legislature to not accept such behavior, and the public has also reacted correctly when it criticized the suspension of payments by liquid companies as lacking solidarity. It is to be hoped that this realization will also be accepted by those companies that currently have a different view of the situation.

CEJ
COMPLIANCE
ELLIANCE
JOURNAL

# RECENT LEGAL DEVELOPMENTS TO ENHANCE CORPORATE LIABILITY FOR CRIMINAL WRONGDOING

Hans-Peter Huber

## AUTHOR

*Hans-Peter Huber, Attorney at Law at Tsambikakis Law Firm, with 40 years of work experience inter alia as senior prosecutor and judge in Munich and General Counsel of Audit and Advisory Firm KPMG Germany has a significant overview on corporate and labor law including all kinds of white collar criminal matters. He is specialized in defending corporations and in conducting noiseless internal investigations either national or international.*

## ABSTRACT

*Due to the coalition agreement of CDU/CSU and SPD the German Government shall implement a new act on corporate criminal liability before the end of the current election period. After an informal draft from the ministry in lead, the BMJV, was leaked to the public this issue is frequently discussed in the media. The author tries to give an overview on the main items of the draft law, the major concerns against it and the mediating draft of the Munich Concept.*

Notwithstanding, that the latest OECD report about the effectiveness of sanctions against companies shows Germany in the upper class of successful enforcement the present political coalition directing Germany had decided in their coalition agreement that a new act about sanctions against corporations shall be developed and pass the parliament before the end of the current election period.

End of August last year the Secretary for Legal Affairs and Consumer Protection (BMJV) had leaked an internal draft of this act to the press. Since then the matter was rather silent up to April 21, when the BMJV contacted all relevant associations and asked for comments until June 12. Attached was an almost unrevised draft and the information that until now there is no harmonized governmental draft agreed from all ministries involved.

On September 6, last year a group of experts led by Professor Saliger from the Munich University and three lawyers frequently asked in white collar crime matters have published a complete draft of a bill about sanctions against corporations including the procedure of internal investigations. They have named their project the Munich Concept (further MC).

They were led by the experience of a legal system in Germany suffering under a tremendous work overload, causing an inacceptable duration of criminal proceedings including the fact that more and more cases become barred due to the statute of limitations. The Government's idea how to handle this critical situation by additionally starting a new line of mandatory investigations without any chance how or where to find experienced staff for the police, the offices of the public prosecutors and also judges may be called ambitious. I am afraid that implementing only this new act in nothing else than an usual pro forma solution, nowadays modern as governmental skill. This will finally be damaging the acceptance of the legal system in our country.

Having laid out these facts at the beginning of this short overview let us now look at the most important aspects of the BMJV Draft and the Munich Concept.

The BMJV draft will be applicable for almost every legal entity in Germany regardless of its statutes of organization or its economic parameters. The German jurisdiction will additionally be extended worldwide as far as international rules allow.

Legal entities shall be held liable for all criminal acts committed by its management or staff this conduct having violated existing legal obligations of the entity or has caused or intended to cause an illicit profit of the entity.

The potential sanctions are fines, a warning with deferred fines or even liquidation of the entity.

For big companies with a business volume of more than 100 Mio Euro p.a. the fine may reach the amount of ten percent of the three years average of the annual worldwide turnover. Even small companies may be charged with fines up to 10 Mio Euro.

Disgorgement of profits from illegal acts will be added to the fines. The fines may be softened if an internal investigation had been conducted and supported the clarification of the facts.

The draft offers some range of flexibility for cases of minor importance by providing options for non or deferred prosecution agreements.

One of the most important political aims is that investigations against companies will be a mandatory obligation of the public prosecutors. As far as I am informed only Spain decided that their authorities shall not have any discretion to decide whether to start an investigation or to dispense.

That being said allow me now to describe the different approach of the MC and the major concerns against the draft of the BMJV.

The principle of mandatory investigations by public prosecutors is an achievement of liberalism in the 2nd part of the 19th century. It was not any longer at the discretion of the aristocracy to decide, whether to commence a criminal investigation or not. The clear legal obligation for the then newly designed and established authority of public prosecutors was to start an investigation on all information about facts which show some clue that a criminal offense might have occurred.

The aim was that at the end of such an investigation there shall be enough evidence to decide whether to indict a suspect or to cease the investigation. The development of penal law since then is nothing less than a continuous increase of criminal offences adding more and more complexity. The staff in the offices of the police and the public prosecutors did not grow simultaneously. The consequence was and still is a significant work overload for the police, for the public prosecutors and for the courts. As all suspects under custody are necessarily handled first, cases of high complexity but without anyone in jail are postponed and the proceedings need more and more time from year to year. The political reaction was that new rules allowed the public prosecutor to cease investigations at their discretion after having conducted a minimum standard of investigations. Since years now this is the most frequent solution of investigations in Germany: the suspension of an investigation after the payment of a fine by the suspect due to an assumed low level of guilt.

As of today the decision to start an investigation against a legal entity is at the discretion of the public prosecutors in Germany. As already mentioned, only Spain is an exemption in Europe and has a mandatory public investigation in corporate wrongdoing. Even after considering the BMJV draft's transition period of two years there will be no chance to build up the experienced resources to solve the high number of additional new mandatory cases which have to be expected in a country with some Million legal entities.

Every country governed by law needs a functioning legal system without bottlenecks as diligent and timely solutions are essential for the citizens' acceptance of this system. To solve this issue the MC votes for a modification of the principle of mandatory proceedings. Those are and will still remain necessary for every individual suspect. The MC allows

the prosecutor to start the investigation against individuals while suspending it against a legal entity until the indispensable individual probe gives significant evidence for an additional corporate wrongdoing. This will be a chance to significantly reduce the immediate need of a second research line against companies.

To avoid an unmanageable increase of proceedings the MC additionally brings an exemption for all legal entities which are small foundations, non-economic, small associations and all those companies which fall under the definition and rules for small and medium sized entities of relevant EU-Law due to their number of employees or their annual turnover.

This exclusion is based also on another important consideration: Many of the rules in the BMJV draft demonstrate the importance of an effective compliance system. But if we take a glance on the compliance directives you cannot deny that all these control mechanisms have been developed for really big companies as a result from lessons learned in the publicly well-known cases like Siemens, Daimler or Volkswagen. Many of these compliance rules overstrain the means of the small and even the middle-sized companies. Mandatory investigations under the scope of such AAA-rules of a so-called sophisticated compliance system will lead to a lethal risk for many of the smaller companies which cannot fulfill all the requirements of this state-of-the-art compliance. The new act will destroy the present system of competition and lead to massive advantages of big entities.

The consequences of such development will not be in the best public interest of a democratic state with a free economy and liberal society.

This matter leads to another issue: Who will feel the sanctions as an unpleasant reaction to an illicit behavior? Who will change its own conduct in order to avoid further sanctions? A legal entity will feel no pain and will not even have an interest so survive. It will always and only be a human being connected and related to the entity, who can show a reaction to punishment. Therefor the MC emphasizes the need not to focus on the companies wrongdoing but to keep constantly the individual liability in mind. It follows the Yates Memorandum from 2015 which until now only slightly altered under the Trump administration

Employees of a company may have participated in a wrongdoing, but on average only a small part of them will have been involved and the majority will be scared to lose their jobs or to get a reduced income due to the fines imposed on their employee. The BMJV draft does not mention the conflicts of interest arising from these facts. Their situation is out of the scope of the new act. How can a government forget or ignore the consequences for innocent workers? Furthermore the shareholders will feel punished without being liable for any individual wrongdoing of the management and in case of public incorporations even without a real chance to influence the company as an owner of for instance 3000 shares. We know since the last financial crisis that the legal consequences of this disaster caused a wide discussion in the USA about the balance between corporate and individual responsibility.

Was this dispute not recognized in our country with such a tradition of work unions and social adjustment? Both groups, employees and shareholders are well recognized in the MC Their situation has to be included in any consideration how to handle a case of corporate liability. Even the works council will have to be involved before imposing fines. And the view on consequences of all sanctions shall also include the effect of fines on other entities which did not where involved in any wrongdoing- The MC tries to mirror the complexity of an economy and shall not focus only on the payment of high fines.

The MC carefully tries to set rules for internal investigations. Internal investigations factually are private investigations. A state governed by law shall not abandon its monopole to take care for legal proceedings in an equal manner for all citizens and entities under its control. If those who are powerful in what way ever will be allowed to conduct their own investigations on their criminal matters the system will finally collapse. Thus the government has to carefully balance the rules under what guidelines private investigations shall be allowed and moreover accepted by public authorities. The MC proposes, that they have to be under scrutiny of the authorities from their planning to their final report. They are not a kind or a part of criminal defense. They are at least a part of the public obligation for a fair trial against everyone. But if the internal investigation follows the rules of an honest cooperation with the authorities they shall be honored. The BMJV draft rules that the defense attorney for a company shall not be conducting an internal investigation. The MC furthermore demands that the internal investigator has to be independent in a similar way as an auditor has to be to allow public reliance in his opinion. But on the other hand, an investigation in full cooperation with the authorities will be absolutely preferred and valued. Only the MC will not allow the seizure of attorney work products as the BMJV draft shall allow thus weakening the confidential position of lawyers without necessity. The MC was until now more or less disdained by the BMJV. Now as the Corona Crisis strikes the economy with inconceivable burden and consequences this new act will have the chance to destroy even those smaller legal entities which have survived the crisis. Let the parliament be reasonable enough to stop and postpone the act which may otherwise be called Corona 2.0. for companies.

CEJ
COMPLIANCE
ELLIANCE
JOURNAL

# EXPERIENCES WITH THE AUSTRIAN ACT ON CORPORATE CRIMINAL LIABILITY ("VERBANDSVERANTWORTLICHKEITS-GESETZ" OR "VbVG")

Heidelinde Luef-Kölbl

## AUTHOR

*Heidelinde Luef-Kölbl is an associate professor at the Institute for Criminal Law, Law of Criminal Procedure and Criminology at the University of Graz, Austria. Her main areas of research include comparative studies of the procedural aspects of white-collar criminal law, especially consensual management strategies for white-collar crime proceedings. Her research activity also focuses on the totality of Austrian criminal procedural law, including its European and international connections.*

## ABSTRACT

*The Austrian Act on Corporate Criminal Liability (VbVG) entered force on 1 January 2006 and has now been in effect fourteen years. The following article will evaluate the VbVG's frequency of application in practice and critically examine the dominance of procedural termination (rather than prosecution) at the discretion of the district attorney's office.*

## TABLE OF CONTENTS

## I. INTRODUCTION

By introducing the Austrian Act on Corporate Criminal Liability (VbVG)[1], which was preceded by a prolonged discussion process[2], the Austrian legislature embarked on new territory in criminal law. Departing from the principle that only natural persons can be prosecuted ("societas delinquere non potest"), the VbVG regulates the conditions under which entities can be held responsible for criminal acts committed within their respective organizational domains.

The VbVG aims to prevent corporate crime. Accordingly, aspects of prevention play a crucial role in the Austrian manifestation of corporate criminal liability.[3] Entities are expected to take active measures to prevent criminal conduct by their employees and those responsible for their executive bodies.[4] The strong nature of the concept of prevention should guarantee protection for victims, make economic life more fair, and strengthen Austria as a place to do business.

By now, any objections raised against the VbVG from the standpoint of constitutional law have been dispelled by the Austrian Constitutional Court (VfGH).[5] The VfGH believes it is permissible to hold an entity responsible for a natural person's unlawful and culpable conduct if they are connected with that entity. Furthermore, the VfGH expressly states that the principle of culpability applies only to natural persons in individual criminal law, but not to entities.

What follows is a brief overview of the VbVG's provisions under criminal law, after which the article will focus on the VbVG's frequency of application while especially considering the role and problem of consensus and cooperation in criminal proceedings against entities.

---

1 BGBl I 151/2005 as ammended by BGBl I 26/2016.

2 For historical development of the statute see: FRITZ ZEDER, VBVG 30 et seq. (2006).

3 Marianne Hilf & Fritz Zeder, *in:* Wiener Kommentar zum Strafgesetzbuch, § 18 VbVG marginal no. 1 (Frank Höpfel & Eckart Ratz, 2nd ed., 2010); Marianne Hilf, *Verfolgungsermessen und Diversion im Verbandsstrafverfahren, in*: Strafprozessrecht im Wandel: Festschrift für Roland Miklau zum 65. Geburtstag 192 (Reinhard Moos et al eds., 2006); Zeder, *Das österreichische Unternehmensstrafrecht (VbVG) – Konzept und erste Erfahrungen*, ANWALTSBLATT 415, 417 (2013).

4 ErläutRV 994 BlgNR 22. GP 34.

5 VfGH 2.12.2016, G 497/2015, G 679/2015.

## II. THE LEGAL FRAMEWORK OF THE VbVG

### A. Conditions for Corporate Liability

For the purposes of § 1 VbVG, "entities" (and therefore those on whom penalties are imposed) means legal entities governed by private or public law, registered partnerships, and European Economic Interest Groupings (EEIGs). Essential criteria for responsibility are that the criminal act be committed by a natural person allocable to the entity (decision maker or employee under § 2 VbVG) either (1) to benefit the entity or (2) in breach of one or more of the entity's obligations (§ 3 VbVG). Criminal acts committed by a decision maker may be directly allocated to the entity, but criminal acts committed by an employee may be allocated to the entity only if that entity has failed to take required organizational measures to prevent such criminal acts.

### B. Sanctions

The entity fine (§§ 4 ff VbVG) is intended as a penalty. It is measured according to the "daily rate" system (meaning the entity's economic capacity), the maximum daily rate being 10,000 euros. The number of daily rates is to be measured by the court under consideration of the severity of the offense (§ 5 VbVG). Since the law prescribes a maximum of 180 daily rates, the pecuniary fine can be no more than 1.8 million euros. Under certain conditions, some or all of the pecuniary fine pronounced is subject to conditional leniency (§§ 6f VbVG).

### C. Alternative Forms of Action ("diversionelle Erledigung")

Not least due to considerations of procedural economy, § 19 VbVG provides for the possibility of (intervening) alternative forms of action ("diversionelle Erledigung") for offenses punishable by prison terms of five years or less. "Alternative" primarily means a "diversion" from the normal response to criminal conduct, a diversion that considerably shortens the respective proceedings. Settling corporate criminal proceedings by way of such a diversion requires that the facts of the case be sufficiently clear. The facts of the case are deemed "sufficiently clear" if a high probability of conviction[6] exists. Moreover, such a diversion is permitted in corporate criminal proceedings only if the proceedings cannot be terminated without consequences and a procedure in accordance with § 18 VbVG (the public attorney's discretion to prosecute[7]) is out of the question. Additional mandatory conditions are the full compensation for the damage and the curing of the act's

6 Hans Valentin Schroll & Robert Kert, *in:* Wiener Kommentar zur Strafprozessordnung, § 198 marginal no. 3 (Helmut Fuchs & Eckart Ratz, 2016); HANNES SCHÜTZ, DIVERSIONSENTSCHEIDUNGEN IM STRAFRECHT 55 (2003).

7 See II. D.

consequences.[8] The public prosecutor's office or the court must also take special and general preventive considerations[9] into account in a procedure in accordance with § 19 VbVG.

In proceedings against entities, paying a monetary amount of fifty daily rates or less, specifying a probational period, and rendering community service are foreseen as alternative measures.

Since the alternative form of action is voluntary, it requires the consent of the entity concerned, which the entity gives by voluntarily assuming the alternative obligations demanded in the offer made by the public prosecutor or the court and (promptly) fulfilling those obligations. Successful alternative forms of action therefore require that a consensus be reached between the entity and the public prosecutor or the court, and effectively end the proceedings.

## D. The District Attorney's Discretion to Prosecute ("Verfolgungsermessen der Staatsanwaltschaft")

One of the most central provisions of the VbVG is probably the legal doctrine of the district attorney's discretion to prosecute, which is standardized in § 18 VbVG and which promotes communication and consensus.[10] This grants the district attorney's office a discretion that exceeds the general options for termination under the Austrian Code of Criminal Procedure.[11] In accordance with the wording under § 18 VbVG as a decision arising from a circumscribed power and not a discretionary decision,[12] the district attorney may refrain or (until the evidence has been collected in the main proceedings) withdraw from prosecuting an entity only after (completely[13]) weighing a series of criteria named by law that make prosecution and sanctions appear unnecessary. The individual criteria that must be weighed concern the minimal socially disruptive value of the offense at hand. But they must always be tied together with considerations of procedural economy and the goal of the punishment. Refraining from prosecution is always excluded, however, if

8 Marianne Hilf & Fritz Zeder, *in:* Wiener Kommentar zum Strafgesetzbuch, § 19 VbVG marginal no. 5 (Frank Höpfel & Eckart Ratz, 2nd ed., 2010).

9 EINHARD STEININGER; VERBANDSVERANTWORTLICHKEITSGESETZ ch. 7 marginal no. 9 (2nd ed., 2018).

10 Heidelinde Luef-Kölbl, *Rolle und Problematik „konsensualer" Verfahrenserledigungen in einem Strafprozess gegen Verbände, in:* Unternehmensstrafrecht 369 (Marianne Lehmkuhl & Wolfgang Wohlers, 2020); Jakob Urbanek, *Verbandsverantwortlichkeit: Die Strafbarkeit von Unternehmen und Verbänden in Österreich – ein Erfolgsmodell?, in:* Das große Handbuch Wirtschaftsstrafrecht 43 et seq. marginal no. 2.142 (Robert Kert & Georg Kodek, 2016).

11 Insofar ascribed FRITZ ZEDER, VBVG 90 (2006) „experimental character" for individual criminal proceedings to this article.

12 Marianne Hilf, *Verfolgungsermessen und Diversion im Verbandsstrafverfahren, in*: Strafprozessrecht im Wandel: Festschrift für Roland Miklau zum 65. Geburtstag 201 (Reinhard Moos et al eds., 2006).

13 A sequence or weighting of the individual criteria concerning their significance is not provided for by statute.

there are general or special preventive reasons for prosecuting the entity, or if such prosecution appears called for in light of a special public interest (§ 18(2) VbVG). Since the scope of application of the discretion to prosecute is not subject to any reduction, the district attorney may in principle refrain from prosecuting any category of offense if the conditions for doing so are met. Admittedly: the criterion of offense severity will set a limit in this case.[14]

Therefore, the option of refraining from prosecuting an entity in accordance with § 18 VbVG primarily serves to relieve the district attorney, the criminal police, and (subsequently) the courts, but especially to protect the economic existence of companies as well.[15]

## III. PRACTICAL SIGNIFICANCE OF THE VbVG

It must be stated in advance that the number of procedural settlements under the VbVG is (still) extremely low when measured against the total number of general procedural settlements by the prosecuting authorities in Austria.[16] This is not least attributable to the hesitant practice of the police regarding criminal charges. [17] However, a continual increase in VbVG proceedings can be recorded in recent years. For example, in 2012 there were only 93 final (substantive) decisions on the merits ("meritorische Entscheidungen")[18], but in 2018 there were already 288.[19] And we can probably assume this upward trend will continue during the next few years.

A study[20] on the VbVG's frequency of application during 2006 to 2011, which was performed five years after the VbVG took effect, essentially showed that corporate criminal

14 Similarly Robert Kert, *Das Verfolgungsermessen im Verbandsstrafrecht*, ZEITSCHRIFT FÜR WIRTSCHAFTS- UND FINANZSTRAFRECHT 70, 71 (2017).

15 Cf. Marianne Hilf & Fritz Zeder, *in:* Wiener Kommentar zum Strafgesetzbuch, § 18 VbVG marginal no. 1 (Frank Höpfel & Eckart Ratz, 2nd ed., 2010); Robert Kert*, Das Verfolgungsermessen im Verbandsstrafrecht*, ZEITSCHRIFT FÜR WIRTSCHAFTS- UND FINANZSTRAFRECHT 70 (2017).

16 Bettina Knötzl, *Von gefährlichen Geschenken & bestechenden Erkenntnissen zu Compliance*, FACHZEITSCHRIFT FÜR WIRTSCHAFTSRECHT („ECOLEX") 554 (2012) believes Austria in a „sleeping beauty slumber" in terms of control corruption.

17 Zeder, *Das österreichische Unternehmensstrafrecht (VbVG) – Konzept und erste Erfahrungen*, ANWALTSBLATT 415, 418 (2013).

18 Without adding substantive decisions such as abruption, separation or other conclusions.

19 Federal Ministry of Justice, security report 2018, p. 32, justiz.gv (Apr. 1, 2020) https://www.justiz.gv.at/home/justiz/daten-und-fakten/berichte/sicherheitsberichte~2c94848525f84a630132fdbd2cc85c91.de.html.

20 WALTER FUCHS ET AL, GENERALPRÄVENTIVE WIRKSAMKEIT: PRAXIS UND ANWENDUNGSPROBLEME DES VERBANDSVERANTWORTLICHKEITSGESETZES (VBVG). EINE EVALUIERUNGSSTUDIE (2001), irks, https://www.irks.at/assets/irks/Publikationen/Forschungsbericht/irks_vbvg_bericht.pdf, (Apr.2, 2020).

proceedings were terminated without consequences with above-average frequency[21] (assuming that they occurred in accordance with § 18 VbVG[22]) and that the ratio of court acquittal was significantly higher than those of other criminal proceedings. The study also showed that district attorneys did not terminate the proceedings as an alternative action (Diversion) as often as they terminated general proceedings in the same manner.[23] This hesitant practice of application in the study is justified, among other reasons, by the fact that criminal prosecution authorities still lacked practical experiences and routines in dealing with the VbVG.[24] But the low frequency of application can also be attributed to reservations felt by the members of the judiciary toward corporate liability.[25]

The fact that nothing in these findings appears to have changed considerably in subsequent years is proven by observing the procedural settlements for VbVG proceedings from 2012 to 2018 as well:[26] Of the (substantive)[27] decisions on the merits ("meritorische Entscheidungen"), in the seven-year average around 80% ended through termination by the prosecuting authorities without consequences.[28] An alternative action was used in around 2% of the cases. The prosecuting authorities pressed charges in around 17% of cases.

In comparison: In general, the rate of termination by the district attorney in Austria in a multi-year average is around 60%, and around 16% of cases end through an alternative action by the district attorney. Around 24% of cases on average are settled by pressing

---

21 WALTER FUCHS ET AL, GENERALPRÄVENTIVE WIRKSAMKEIT: PRAXIS UND ANWENDUNGSPROBLEME DES VERBANDSVERANTWORTLICHKEITSGESETZES (VBVG). EINE EVALUIERUNGSSTUDIE 74 et seq. (2001), irks (Apr.2, 2020) https://www.irks.at/assets/irks/Publikationen/Forschungsbericht/irks_vbvg_bericht.pdf.

22 WALTER FUCHS ET AL, GENERALPRÄVENTIVE WIRKSAMKEIT: PRAXIS UND ANWENDUNGSPROBLEME DES VERBANDSVERANTWORTLICHKEITSGESETZES (VBVG). EINE EVALUIERUNGSSTUDIE 3 (2001), irks (Apr.2, 2020) https://www.irks.at/assets/irks/Publikationen/Forschungsbericht/irks_vbvg_bericht.pdf.

23 WALTER FUCHS ET AL, GENERALPRÄVENTIVE WIRKSAMKEIT: PRAXIS UND ANWENDUNGSPROBLEME DES VERBANDSVERANTWORTLICHKEITSGESETZES (VBVG). EINE EVALUIERUNGSSTUDIE 3 et seq. (2001), irks (Apr.2, 2020) https://www.irks.at/assets/irks/Publikationen/Forschungsbericht/irks_vbvg_bericht.pdf.

24 WALTER FUCHS ET AL, GENERALPRÄVENTIVE WIRKSAMKEIT: PRAXIS UND ANWENDUNGSPROBLEME DES VERBANDSVERANTWORTLICHKEITSGESETZES (VBVG). EINE EVALUIERUNGSSTUDIE 4 (2001), irks (Apr.2, 2020) https://www.irks.at/assets/irks/Publikationen/Forschungsbericht/irks_vbvg_bericht.pdf.

25 WALTER FUCHS ET AL, GENERALPRÄVENTIVE WIRKSAMKEIT: PRAXIS UND ANWENDUNGSPROBLEME DES VERBANDSVERANTWORTLICHKEITSGESETZES (VBVG). EINE EVALUIERUNGSSTUDIE 112 et seq. (2001), irks (Apr.2, 2020) https://www.irks.at/assets/irks/Publikationen/Forschungsbericht/irks_vbvg_bericht.pdf.

26 The following numbers are based on the statistical numbers of Federal Ministry of Justice, security report 2018, 32 justiz.gv (Apr. 1, 2020) https://www.justiz.gv.at/home/justiz/daten-und-fakten/berichte/sicherheitsberichte~2c94848525f84a630132fdbd2cc85c91.de.html, on own calculations and may vary in total from 100 % due to roundings.

27 Therefore, this is without taking the non-substantive decisions into account, which accounted for 21 % of the cases in this period under observation.

28 Whereas the proceeding against accused natural persons, at the same time as the entities, were terminated in only about 64 % of the cases, cf. Richard Soyer & Stefan Schumann, *Die „Frankfurter Thesen" zum Unternehmensstrafecht unter Einbeziehung der Erfahrungen in Österreich*, ZEITSCHRIFT FÜR WIRTSCHAFTS- UND STEUERSTRAFRECHT („WISTRA") 321, 324 (2018).

charges.[29] This shows that the trend of the first five years has continued, and that termination rates in proceedings against entities are above average, probably owing mostly to the district attorney's far-reaching discretion to prosecute under § 18 VbVG.[30] However, the displacement effect caused by the alternative form of action through the discretion to prosecute can also be recognized.[31] This is worrying primarily regarding the principle of searching for substantive truth, since sufficient clarity of the facts of the case is demanded when alternative forms of action are taken, but this condition is lacking for proceedings in accordance with § 18 VbVG.

Furthermore, during proceedings against entities, the procedure of the courts clearly deviates from the general picture. Although the average long-term acquittal rate from the courts lies around 15%[32], main proceedings against entities end with an acquittal in around 36% of cases on average (2012–2018). The rate of conviction generally lies at over 50% on average[33], but only 35% on average for corporate criminal proceedings during a seven-year period. With alternative forms of action, on the other hand, around 16% of corporate criminal proceedings are ended by the courts like the general proceedings. These findings also support the proposition outlined above: that alternative forms of action are displaced through the district attorney's discretion to prosecute.

In the result, it can be stated that the district attorney's discretion to prosecute takes on a disproportionately high role during criminal proceedings against entities.[34] One possible reason for this, among others, is the continuing skepticism that judicial bodies harbor against corporate criminal liability. But the additional expense that criminal prosecution authorities must incur for criminal proceedings against an entity, while facing inadequate opportunity for sanctions and a permanent scarcity of resources, also does its part to keep the Austrian Act on Corporate Criminal Liability from being applied more than hesitantly and the termination rate significantly higher than those of general proceedings.[35]

---

29 Federal Ministry of Justice, *security report 2018*, justiz.gv (Apr. 1, 2020) https://www.justiz.gv.at/home/justiz/daten-und-fakten/berichte/sicherheitsberichte~2c94848525f84a630132fdbd2cc85c91.de.html.

30 Zeder, *Das österreichische Unternehmensstrafrecht (VbVG) – Konzept und erste Erfahrungen*, ANWALTSBLATT 415, 417 (2013).

31 This was already feared in the development of the statute: cf. FRITZ ZEDER, VBVG 91 (2006).

32 Last for 2018: 17 % (source: ministry of the interior, *security report 2018*, 21, bmi.gv,, (Apr. 02, 2020), https://www.bmi.gv.at/508/files/SIB_2018/4_SIB_2018_BMVRDJ_web.pdf.

33 Last for 2018: 56,7 % (source: ministry of the interior, security report 2018, 21, bmi.gv,, (Apr. 02, 2020), https://www.bmi.gv.at/508/files/SIB_2018/4_SIB_2018_BMVRDJ_web.pdf.

34 Similarly Lyane Sautner, *Grundlagen und Herausforderungen der strafrechtlichen Verantwortlichkeit juristischer Personen in Österreich*, ÖSTERREICHISCHE JURISTENZEITUNG (ÖJZ) 551 (2012).

35 Zeder, *Das österreichische Unternehmensstrafrecht (VbVG) – Konzept und erste Erfahrungen*, ANWALTSBLATT 415, 418 (2013).

## IV. PRINCIPLE OF LEGALITY VERSUS OPPORTUNITY

According to the view expressed in the legal materials on the Austrian Act on Corporate Criminal Liability, the district attorney's discretion to prosecute is indeed a "regulation of opportunity,"[36] but one which does not oppose the principle of legality which applies in the VbVG.[37] On the other hand, the literature repeatedly expresses the view that the district attorney's discretion to prosecute under § 18 VbVG is not a regulation of appropriateness, but should be deemed only an additional, legally determined alternative action that the district attorney may take[38] or a (mere) restriction of the principle of legality .[39]

However, the district attorney's discretion to prosecute does not appear unproblematic. The frequency of application of § 18 VbVG raises the question of whether the State's right to inflict punishment can still be asserted in corporate proceedings, thereby constituting effective combat against criminality in associations and companies. Since the termination of proceedings under § 18 VbVG is not subject to the courts' control, the district attorney's procedure is mostly nontransparent. At the same time, the frequency of application underscores the dominant role the district attorney plays in criminal proceedings against entities, since the district attorney alone may decide whether or not to avail itself of its discretion to prosecute. Admittedly, it may not decide arbitrarily, but is bound by a discretion that arises from circumscribed powers by means of the prescribed criteria. However, this does not entitle the prosecuted entity to any subjective right to termination under § 18 VbVG.[40] And not least, such terminations carried out by the district attorney must also satisfy the determinants of the principle of equality, under which any unequal treatment of accused parties must be strictly justified in fact.[41] Therefore, improper terminations would oppose the principle of legality.

---

36 Similarly Zeder, *Das österreichische Unternehmensstrafrecht (VbVG) – Konzept und erste Erfahrungen*, ANWALTSBLATT 415, 416 (2013); Jakob Urbanek, *Verbandsverantwortlichkeit: Die Strafbarkeit von Unternehmen und Verbänden in Österreich – ein Erfolgsmodell?, in*: Das große Handbuch Wirtschaftsstrafrecht 43 et seq. marginal no. 2.133 (Robert Kert & Georg Kodek, 2016).

37 ErläutRV 994 BlgNR 22. GP 34; also Richard Soyer & Stefan Schumann, *Die „Frankfurter Thesen" zum Unternehmensstrafecht unter Einbeziehung der Erfahrungen in Österreich*, ZEITSCHRIFT FÜR WIRTSCHAFTS- UND STEUERSTRAFRECHT („WISTRA") 321, 324 (2018) talk about an expediency article.

38 Marianne Hilf & Fritz Zeder, *in*: Wiener Kommentar zum Strafgesetzbuch, § 18 VbVG marginal no. 4 (Frank Höpfel & Eckart Ratz, 2nd ed., 2010); Robert Kert, *Umfang und Grenzen des Opportunitätsprinzips im Verbandsstrafrecht, in:* Finanzstrafrecht 2016 197 et seq. (Roman Leitner & Rainer Brandl, 2017); EINHARD STEININGER; VERBANDSVERANTWORTLICHKEITSGESETZ ch. 9 marginal no. 9 et seq. (2nd ed., 2018); Einhard Steininger, *Die Neuorientierung des strafprozessualen Legalitätsprinzips*, JURISTISCHE BLÄTTER (JBl) 289, 298 (1986).

39 Richard Soyer, *Gerechtigkeit – Absprachen – Korruption*, JOURNAL FÜR STRAFRECHT (JSt) 37, 42 (2013).

40 Bettina Knötzl, *Von gefährlichen Geschenken & bestechenden Erkenntnissen zu Compliance*, FACHZEITSCHRIFT FÜR WIRTSCHAFTSRECHT („ECOLEX") 554 (2012) demands a subjective right to termination of the proceeding for the entity.

41 Einhard Steininger, *Die Neuorientierung des strafprozessualen Legalitätsprinzips*, JURISTISCHE BLÄTTER (JBl) 289, 298 (1986).

## V. COOPERATION AS A PREREQUISITE FOR PROCEEDINGS IN ACCORDANCE WITH §§ 18 AND 19 VbVG

Since a termination of proceedings in accordance with § 18 or 19 VbVG usually comes into question only if the entity exhibits positive conduct after the offense (by paying damages[42], helping to clear up the case through internal investigations[43], or subsequently introducing compliance programs[44], for example), it is recognizable that those termination options are closely interwoven with the entity's willingness to cooperate.[45] Moreover, companies are often willing to cooperate, since they have an economic interest in avoiding investigative procedures and a guilty verdict in accordance with the VbVG, and especially in being associated with as little negative publicity as possible.[46] The VbVG's general preventive effect is not least attributable to a company's fear of negative media reports regarding corporate criminal proceedings conducted against that company.[47] However, practice shows that companies do not usually fear being fined as an entity.[48] With a maximum limit of 1.8 million euros, such fines aren't a great deterrent to companies. The first time an entity is convicted, courts usually pronounce only 20% to 30% of the penalty

42 Cf. Heidelinde Luef-Kölbl, *Rolle und Problematik „konsensualer" Verfahrenserledigungen in einem Strafprozess gegen Verbände, in*: Unternehmensstrafrecht 397 (Marianne Lehmkuhl & Wolfgang Wohlers, 2020).

43 On the topic and difficulty of internal investigations in more detail among others Norbert Wess & Markus Machan, *Zum Anwaltsprivileg im Rahmen von unternehmensinternen Ermittlungen, in*: Jahrbuch Wirtschaftsstrafrecht und Organverantwortlichkeit 2017 58 (Peter Lewisch, 2017); Lukas Staffler, *Internal Investigations und nemo tenetur*, ZEITSCHRIFT FÜR WIRTSCHAFTS- UND FINANZSTRAFRECHT (ZWF) 174 (2018); Patrick Madl, *Unternehmensinterne Untersuchungen im Wirtschaftsstrafverfahren, in*: Das große Handbuch Wirtschaftsstrafrecht 815 et seq. (Robert Kert & Georg Kodek, 2016); Norbert Wess, *Unternehmensinterne Ermittlungen – Erfahrungen und Problemstellungen in Österreich*, ANWALTSBLATT (AnwBl) 223 (2013).

44 Cf. „Compliance" as a group of themes in general among others Richard Soyer & Sergio Pollak, *Compliance: Mehr als ein Mode(Zauber-)Wort, in*: Das große Handbuch Wirtschaftsstrafrecht 1013 et seq. (Robert Kert & Georg Kodek, 2016).

45 Cf. in more detail Heidelinde Luef-Kölbl, *Rolle und Problematik „konsensualer" Verfahrenserledigungen in einem Strafprozess gegen Verbände, in*: Unternehmensstrafrecht 371 et seq. (Marianne Lehmkuhl & Wolfgang Wohlers, 2020).

46 Michael Rohregger & Norbert Wess, *Verbandsverantwortlichkeitsgesetz, in*: Praktikerkommentar Wirtschaftsstrafrecht § 1 VbVG marginal no. 7 (Mathias Preuschl & Norbert Wess 2018).

47 WALTER FUCHS ET AL, GENERALPRÄVENTIVE WIRKSAMKEIT: PRAXIS UND ANWENDUNGSPROBLEME DES VERBANDSVERANTWORTLICHKEITSGESETZES (VBVG). EINE EVALUIERUNGSSTUDIE 124 (2001), irks (Apr.2, 2020) https://www.irks.at/assets/irks/Publikationen/Forschungsbericht/irks_vbvg_bericht.pdf.

48 Norbert Wess et al, *(Neben-)Folgen einer Verurteilung nach dem VbVG*, ZEITSCHRIFT FÜR WIRTSCHAFTS- UND FINANZSTRAFRECHT (ZWF) 54, 55 (2017); Norbert Wess & Markus Machan, *Zum Anwaltsprivileg im Rahmen von unternehmensinternen Ermittlungen, in:* Jahrbuch Wirtschaftsstrafrecht und Organverantwortlichkeit 2017 58 (Peter Lewisch, 2017); Zeder, *Das österreichische Unternehmensstrafrecht (VbVG) – Konzept und erste Erfahrungen*, ANWALTSBLATT 415, 417 (2013).

range.[49] Far more threatening for companies are the incidental legal consequences[50] that judicial sentencing might bring, such as being sued for damages under civil law or banned from participating in public tenders[51]. Moreover, the loss of reputation tied to a conviction[52] can impair future transactions and the trust of customers or suppliers.[53] Therefore, defence lawyers also use cooperative behaviour[54] as a strategic means for convincing the criminal prosecution authorities that the conditions for terminating proceedings in accordance with §§ 18 or 19 VbVG have been met. However, the companies' interest in self-preservation[55] may not blind us to the fact that there is a fine line between willingness to cooperate and an obligation to cooperate, especially where avoiding a conviction is concerned.[56]

## VI. CONCLUSION

The introduction of the Austrian Act on Corporate Criminal Liability was seen as a paradigm shift within Austrian criminal law.[57] That estimation applies not least to the broadness of the district attorney's discretion to prosecute, which far exceeds the termination options under the Austrian Code of Criminal Procedure and is based on the preventive orientation of the VbVG.[58] Together with the option of termination through an alterna-

---

49 Norbert Wess & Markus Machan, *Zum Anwaltsprivileg im Rahmen von unternehmensinternen Ermittlungen, in*: Jahrbuch Wirtschaftsstrafrecht und Organverantwortlichkeit 2017 58 (Peter Lewisch, 2017).

50 Jakob Urbanek, *Verbandsverantwortlichkeit: Die Strafbarkeit von Unternehmen und Verbänden in Österreich – ein Erfolgsmodell?, in*: Das große Handbuch Wirtschaftsstrafrecht 43 et seq., marginal no. 2.118, 2.193, (Robert Kert & Georg Kodek, 2016).

51 Jakob Urbanek, *Verbandsverantwortlichkeit: Die Strafbarkeit von Unternehmen und Verbänden in Österreich – ein Erfolgsmodell?, in*: Das große Handbuch Wirtschaftsstrafrecht 43 et seq., marginal no. 2.116 (Robert Kert & Georg Kodek, 2016).

52 Jakob Urbanek, *Verbandsverantwortlichkeit: Die Strafbarkeit von Unternehmen und Verbänden in Österreich – ein Erfolgsmodell?, in*: Das große Handbuch Wirtschaftsstrafrecht 43 et seq., marginal no. 2.118, 2.144 (Robert Kert & Georg Kodek, 2016).

53 Zeder, *Das österreichische Unternehmensstrafrecht (VbVG) – Konzept und erste Erfahrungen*, ANWALTSBLATT 415, 418 (2013); Lukas Staffler, *Internal Investigations und nemo tenetur*, ZEITSCHRIFT FÜR WIRTSCHAFTS- UND FINANZSTRAFRECHT (ZWF) 174 (2018).

54 Cf. Alexia Stuefer, *Strategien der Verteidigung in Wirtschaftsstrafsachen, in:* Das große Handbuch Wirtschaftsstrafrecht 895 et seq., marginal no. 24.32 (Robert Kert & Georg Kodek, 2016).

55 Amr Sarhan, *Wie viel Kooperation zwischen Unternehmen und der Strafjustiz bei der Aufklärung verbandsinterner Kriminalität verträgt der Strafprozess?*, ZEITSCHRIFT FÜR WIRTSCHAFTS- UND STEUERSTRAFRECHT (WISTRA) 336, 337 (2017).

56 Jakob Urbanek, *Verbandsverantwortlichkeit: Die Strafbarkeit von Unternehmen und Verbänden in Österreich – ein Erfolgsmodell?, in:* Das große Handbuch Wirtschaftsstrafrecht 43 et seq. marginal no. 2.144 (Robert Kert & Georg Kodek, 2016) believes to see "the picture of the hold-up carrot" in § 18 VbVG.

57 FRITZ ZEDER, VBVG 3 (2006).

58 ErlRV 994 BlgNR 22. GP 34.

tive form of action, this strongly encourages a company to cooperate if investigative proceedings are initiated against an entity in accordance with the VbVG.[59] From the standpoint of the entity concerned, consensual settlement of the criminal proceedings gives them an opportunity to avoid a conviction (and the associated risk of farther-reaching financial loss) and to minimize damage. Cooperative conduct pays off for the entity, since all the incentives standardized under the law can allow them to expect either more lenient treatment when their fine is assessed or even the termination of the proceedings without consequences. It also allows the criminal prosecution authorities to end the criminal proceedings efficiently while preserving resources. And not least, the focus on cooperation and communication corresponds to the VbVG's preventive orientation, and future-focused preventive mechanisms can in many cases make a greater contribution to rehabilitating the entity than can repressive reactions to criminal conduct.[60]

The clear dominance of the terminations without consequences under § 18 VbVG in proceedings during corporate criminal offenses is surprising, however, since, although this regulation serves the companies' economic existence and provides advantages in terms of procedural economy, it also entails risks for criminal justice — especially regarding the search for substantive truth.

59 The Austrian Constitutional Court (Verfassungsgerichtshof) decided, as part of his validation if the Austrian Act on Corporate Criminal Liability (VbVG, VfGH 2.12.2016, G 497/2015, G 679/2015) is in conformity with the constitution, that the sanction system with reference to §§ 18 and 19 VbVG is appropriate and proportionate.

60 Rainer Brandl & Roman Leitner, *Bestrafung von Verbänden für Finanzvergehen (Teil II)*, STEUER UND WIRTSCHAFTSKARTEI (SWK) 980, 983 et seq. (2018).

CEJ
COMPLIANCE
ELLIANCE
JOURNAL

# SWISS LEGAL STATUS ON THE PROTECTION OF WHISTLE-BLOWERS[1]

Taking into account the EU Directive on the protection of persons who report breaches of Union law.

Rita Pikó

## AUTHOR

*Dr. Rita Pikó, LL.M. (Exeter), lectures in compliance at the Zurich University of Applied Sciences (ZHAW) and is the head (Studienleiterin) of the CAS Compliance Investigator degree program. She is an attorney at law in Zurich in her law firm Pikó Uhl Rechtsanwälte AG, admitted in Switzerland and Germany and specialized in corporate compliance and internal investigations. Dr. Pikó is a regular speaker at the qualification program for supervisory board members (Exzellenzprogramm für Aufsichtsräte) at the Frankfurt School of Management & Finance.*

## ABSTRACT

*The EU Whistleblower Protection Directive came into force on 16 December 2019. Switzerland continues to struggle with this topic: the Swiss National Council (Nationalrat) dismissed a draft law on its introduction on 3 June 2019 and, after the Swiss Council of States (Ständerat) approved the draft law without changes on 16 December 2019, dismissed it again on 5 March 2020.*

---

1 This Article has been first published in German at the Compliance Berater (Vol. 7) 2019, p. 235-242. The Author is very grateful to the Compliance Berater for allowing her to publish this translation including an update.

## TABLE OF CONTENTS

## I. INTRODUCTION

Whistleblowing and the protection of whistleblowers matters in the fight against national and international economic crime. According to an ACFE study, 40% of all cases of occupational fraud are identified by reports from whistleblowers, 53% of which are employees.[2] A survey of companies in Switzerland also showed that a whistle-blowing system allowed half of them to uncover between 21% to 60% of their total financial losses.[3] The European Parliament passed the EU Directive on the protection of persons who report breaches of Union law (EU Whistleblower Protection Directive) on 16 April 2019. The directive came into force on 16 December 2019.[4] The EU Member States are obliged to incorporate these regulations within two years of publication of the directive into their respective national laws.

To date, the explicit protection of whistleblowers has not yet been regulated in Switzerland, with the exception of Art. 22a of the Swiss Federal Personnel Act (*Bundespersonalgesetz*), and respective cantonal regulations on personnel. Accordingly, there is a lack of legal certainty for employers as well as employees in particular, as the principles for the protection of whistleblowers developed by court rulings are not sufficient. For this reason, Switzerland is evaluated by the OECD as *insufficient* in respect of the legal protection of whistleblowers.[5] Apart from the lack of a fundamental protection of whistleblowers, among others, the OECD criticizes the lack of sanctions for those who take retaliation measures against a whistleblower and the lack of regulations on securing the confidentiality of reports and protecting the whistleblower's identity from being disclosed.[6] The gap in statutory law regarding the legal protection of whistleblowers was meant to be closed by a law on the protection of whistleblowers. However, the draft law was clearly rejected by the Swiss National Council (*Nationalrat*) on 3 June 2019 by 144 to 27 votes and again on

2 ACFE, Report to the Nations on Occupational Fraud and Abuse, 2018 Global Fraud Study, 17 (2 Mar., 2020) https://www.acfe.com/report-to-the-nations/2018/.

3 Christian Hauser, Nadine Hergovits & Helene Blumer, *Whistleblowing Report 2019*, Chur 2019, 61.

4 DIRECTIVE (EU) 2019/1937 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 October 2019 on the protection of persons who report breaches of Union law, OFFICIAL JOURNAL OF THE EUROPEAN UNION, L 305, 17, (2 Mar., 2020) https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L1937&from=EN.

5 The OECD report dated 15.3.2018 states: "The examiners recommend that Switzerland adopt urgently an appropriate regulatory framework to compensate and protect private sector employees who report suspicions of foreign bribery from any discriminatory or disciplinary action. (...) Finally, the examiners recommend that the Working Group should follow up on prosecutions brought in Switzerland against whistleblowers who report suspected financial offences including, in particular, foreign bribery." OECD, Implementing the OECD Anti-Bribery Convention, Phase 4 Report: Switzerland, page 13 et seq.; (2 Mar., 2020) https://www.oecd.org/corruption/anti-bribery/Switzerland-Phase-4-Report-ENG.pdf.

6 OECD Anti-Bribery Convention, Phase 4 Report: Switzerland (15 March 2018), 16.

5 March 2020 by 147 to 42 votes.[7]

## II. HISTORY

Switzerland has been discussing the protection of whistleblowers and several draft laws for over a decade. As early as 22 June 2007 the Swiss parliament passed the Gysin motion "Statutory protection of whistleblowers from corruption" (No. 03.3212). On 5 December 2008 the Swiss Federal Council (*Bundesrat*) submitted the first pre-draft of the partial revision of the Swiss Code of Obligations (CO) for consultation, and the Federal Department of Justice and Police (FDJP) developed a bill for the consultation process. On 1 October 2010 a pre-draft for the partial revision of the CO on the sanctions of abusive or unjustified notice was opened.[8] The Swiss Federal Council (*Bundesrat*) submitted a report on the partial revision of the CO to the parliament on 20 November 2013[9] which the Swiss Council of States (*Ständerat*) accepted with few amendments on 22 September 2014. On 5 May 2015, however, the Swiss National Council (*Nationalrat*) clearly rejected the submission by 134 to 49 votes and instructed the Swiss Federal Council (*Bundesrat*) to phrase the draft more clearly and simply.[10] The Swiss Council of States (*Ständerat*) unanimously agreed to the rejection of the submission.[11] After this lengthy history the Swiss Federal Council (*Bundesrat*) affirmed anew its intention to legislate whistleblowing. The council then passed an amended draft[12] (CH-Draft-CO) and a corresponding additional report, preserving the principles of the preceding version,[13] on 21 September 2018.

As both the Swiss National Council (*Nationalrat*) and the Swiss Council of States (*Ständerat*) engaged in the draft law, the legislative process was formally in the procedure of reconciling after the first refusal by the Swiss National Council (*Nationalrat*) on 3 June 2019. The Swiss Council of States (*Ständerat*), however, did not follow the Swiss National Council (*Nationalrat*) and approved the draft law without changes on 16 December 2019.

---

7 Results of the voting as of 3.6.2019, viewed on 2.3.2020 under: https://www.parlament.ch/de/ratsbetrieb/amtliches-bulletin/amtliches-bulletin-die-verhandlungen?SubjectId=46133#votum21 x respectively results of the voting as of 5 March 2020, viewed on 13 March 2020 under: https://www.parlament.ch/de/ratsbetrieb/amtliches-bulletin/amtliches-bulletin-die-verhandlungen?SubjectId=48524#votum13.

8 See Diana Imbach Haumüller, *Whistleblowing in der Schweiz und im internationalen Vergleich – ein Bestandteil einer effektiven internen Kontrolle?* Diss. Universität Zürich, Zürich/Basel/Genf 2011; Diana Imbach Haumüller, Whistleblowing – *Bestandteil einer effektiven internen Kontrolle*, GesKR 2013, 71 et seq.; Nicole Jungo, *Whistleblowing – Lage in der Schweiz*, recht. 2012, 65, 72 et seq.

9 BBl 2013 9513.

10 See Sara Licci, *Codes of Conduct im Arbeitsverhältnis mit besonderem Blick auf das Whistleblowing*, AJP 2015, 1168.

11 See the summary of the starting position in: Additional Report to the partial revision of the Swiss Code of Obligations (*Zusatzbotschaft zur Teilrevision des Obligationenrechts (Schutz bei Meldung von Unregelmässigkeiten am Arbeitsplatz*) as of 21 September 2018 (*Zusatzbotschaft*), BBl 2019 1409, 1411 et seq.

12 The File Number of CH-Draft-CO is 13.094 published at BBl 2019 1433 et seq.

13 Additional Report (*Zusatzbotschaft*), BBl 2019 1409 et seq.

The draft law was therefore resubmitted to the Swiss National Council (*Nationalrat*). The Legal Affairs Committee of the Swiss National Council (*Nationalrat*) advised its council in January 2020 to stick to its resolution and not to enter into the submission.[14] Unsurprisingly, the draft law was again dismissed by the Swiss National Council (*Nationalrat*) on 5 March 2020, with the consequence that the submission is now definitely rejected.

## III. THE SWISS DRAFT LAW IN LIGHT OF THE EU WHISTLEBLOWER PROTECTION DIRECTIVE

### A. Regulatory Approach

Pursuant to a current study, a large part of Swiss companies, i.e. 71.2% of large Swiss companies and 50.5% of SMEs with 20 to 249 employees, have – without any statutory obligation – already incorporated a reporting office for whistleblowers. The reasons for the incorporation of a reporting office by these Swiss companies are, in particular, to strengthen a corporate image of ethics and integrity and to avoid financial damages; but the move is also driven by an intrinsic conviction of the benefit and efficiency of a reporting office. The most important reasons cited for not setting up a reporting office were the absence of any statutory obligation and the intention to avoid a culture of denunciation.[15]

Despite the introduction of whistleblowing systems by Swiss companies already being far advanced, the Swiss Federal Council (*Bundesrat*) proposed to introduce statutory regulations on this topic. Through these regulations the Swiss Federal Council (*Bundesrat*) aimed to procure legal certainty in all areas. The following describes the CH-Draft-CO as proposed to the Swiss National Council (*Nationalrat*).

Employees obtain the right to report[16] and, in safeguarding their fiduciary duty under labor law, shall receive clarity on the conditions under which they may make a report. By this the reporting is legitimized. The employer, when introducing internal whistleblowing systems, shall receive clarity on which procedures must be complied with to reduce the risk that their employees will make reports to authorities or to the public. The CH-Draft-CO thereby proposes legal *incentives* instead of a statutory duty to implement an internal reporting office.

---

14 Media release of the Legal Commission of the Swiss National Council as of 31 January 2020; (2 Mar., 2020) https://www.parlament.ch/press-releases/Pages/mm-rk-n-2020-01-31.aspx.

15 Christian Hauser, Nadine Hergovits & Helene Blumer, *Whistleblowing Report 2019*, Chur 2019, 17, 18 and 20.

16 The question whether employees are subject to a duty to report irregularities is not addressed in this article. In that respect see Diana Imbach Haumüller, *Whistleblowing in der Schweiz und im internationalen Vergleich – ein Bestandteil einer effektiven internen Kontrolle?* Diss. Universität Zürich, Zürich/Basel/Genf, 2011 Rn. 73; Sara Licci, *Codes of Conduct im Arbeitsverhältnis mit besonderem Blick auf das Whistleblowing*, AJP 2015, 1168, 1180.

In contrast to the CH-Draft-CO, the EU Whistleblower Protection Directive obliges corporates and communities that provide for a certain size to implement whistleblowing systems and determines minimum standards.

## B. Personal Scope of Application

The CH-Draft-CO applies to reports in the context of employment relationship in the private sector. For this reason, the protection of whistleblowers shall be incorporated into the Swiss Code of Obligations (*Obligationenrecht*, CO). The regulations of the CH-Draft-CO shall be embedded in connection with the fiduciary duty of an employee towards his or her employer and the obligation to secrecy resulting therefrom, pursuant to Art. 321a CO (Art. 321a$^{bis\,0}$ et seq. CH-Draft-CO).

Accordingly, voluntary, pro bono and retired employees and self-employed persons do not fall within the scope of application. The Swiss Federal Personnel Act (*Bundespersonalgesetz*, BPG)[17] applies to public service employees and regulates in Art. 22a BPG the right and the duty to report in the case of detected grievances.[18] Customers, suppliers, shareholders and other stakeholders with no employment relationship with the corporation also do not fall within the scope of application of the CH-Draft-CO, and nor do third parties who often are permitted to report within the whistleblowing systems of large international groups.

In practice, Swiss enterprises offer, in addition to their employees, further groups of persons the possibility to use their reporting office. These groups include, among others, customers (40.6%), shareholders (22.4%), employees of suppliers (22.4%) or competitors (13%).[19]

The protection under the EU Whistleblower Protection Directive, in contrast, is not limited to the private sector but, pursuant to Art. 4, also includes public law employment relationships (including public officials) as well as the self-employed within the meaning of Art. 49 TFEU, shareholders and persons belonging to the administrative, management or supervisory body of an enterprise, including non-executive members, as well as volunteers, trainees, and persons working under the supervision and direction of contractors and suppliers. In addition, the protective measures also apply to facilitators and third parties such as colleagues and relatives of the whistleblower.

A further difference between the CH-Draft-CO and the EU Whistleblower Protection Directive is as follows: The EU Whistleblower Protection Directive leaves it up to the individual member state's law whether the duty to implement reporting channels applies

17 BPG, SR 172.220.1.

18 The BPG is not addressed any further in this article. In that respect see Nicole Jungo, *Whistleblowing – Lage in der Schweiz*, recht. 2012, 65, 68 et seq.

19 Christian Hauser, Nadine Hergovits & Helene Blumer, *Whistleblowing Report 2019*, Chur 2019, 38.

only to employers with 50 or more employees, or respectively to communities of more than 10,000 inhabitants (Art. 8)[20]. Enterprises in the financial services sector are obliged to implement the channels irrespective of their size (Art. 8 (4)).[21] The CH-Draft-CO does not provide for such distinctions, with the result that the regulations apply in theory from one employee and upwards; the draft, however, does not impose a duty to implement reporting channels.

## C. Material Scope of Application

At present there is legal uncertainty in Switzerland for employees regarding whether and to whom at their place of employment they may report irregularities without breaching their fiduciary duty (Art. 321a para. 4 CO) and whether they render themselves liable to prosecution by doing so (Art. 162 Swiss Criminal Code (CH-StGB)).[22] The CH-Draft-CO addresses these aspects and states the conditions under which employees may lawfully report irregularities while respecting their fiduciary duty under labor law.

In line with this logic, the supplementary report rules that compliance with the conditions for a report qualifies as a statutory justification in the meaning of Art. 41 CH-StGB. A whistleblower acting in compliance with the regulations of the CH-Draft-CO is therefore not threatened by sanctions under criminal law.[23]

### 1. Irregularities

Pursuant to Art. 321a$^{bis\ 0}$ CH-Draft-CO, employees may report irregularities. Criminal acts, breaches of statutory law, and violations of internal regulations of the employer (Art. 321a$^{bis\ 0}$ para. 2 CH-Draft-CO)[24] that come within the confidentiality duty of the employee resulting from the employment relationship (Art. 321a para. 4 CO) qualify as irregularities. This includes all confidential facts the employee learns of while in the service of the employer, in particular industrial and business secrets as well as all other facts which

---

20 The regulation contained in the draft version of the EU Whistleblower Protection Directive pursuant to which the obligation applies only to civil law entities with an annual turnover or an annual balance of more than EUR 10 million is no longer part of the passed version.

21 Based on a risk assessment, Member State rules may also oblige entities from other sectors to implement reporting systems, irrespective of their size (recital 48), and to incentivize smaller entities below the minimum size to implement reporting systems (e.g. by reducing the requirements) (recital 49); P8_TA-PROV(2019)0366, p. 32.

22 Art. 162 CH-StGB states: "Any person who betrays a manufacturing or trade secret that he is under a statutory or contractual duty contract not to reveal, any person who exploits for himself or another such a betrayal, is liable on complaint to a custodial sentence not exceeding three years or to a monetary penalty."; Swiss Criminal Code, SR 311.0 (CH-StGB).

23 Additional Report (*Zusatzbotschaft*), BBl 2019 1409, 1414.

24 This listing is not exhaustive; Additional Report (*Zusatzbotschaft*), BBl 2019 1409, 1416.

the employer under certain circumstances wants to be kept confidential.[25] Facts that are not subject to this confidentiality duty do not meet the conditions for a legitimate report pursuant to Art. 321a$^{bis\,0}$ para. 2 CH-Draft-CO.[26]

The term "irregularity" is partially non-mandatory law[27] on the first level of cascade[28]. This because the employer may determine, in addition to violations of criminal and administrative law and other statutory regulations which are verifiable by authorities, that further violations (e.g. of internal regulations) qualify as irregularities in the meaning of Art. 321a$^{bis\,0}$ CH-Draft-CO. It is therefore at the discretion of the employer to determine in the corporate code of conduct what additional cases may be reported, such as cases of discrimination or sexual harassment. Irregularities that may be reported to authorities or that may be disclosed to the public are exclusively defined by law, however, and therefore do not fall within the non-mandatory category.[29]

The material scope of application of the EU Whistleblower Protection Directive governs the minimum standard applicable to all EU Member States by referring to breaches of EU law in the categories listed in Art. 2. These include, in particular, public procurement, financial services, financial products and financial markets, the prevention of money laundering and financing of terrorism, product safety, environmental protection, food safety, public health, customer protection, protection of privacy and personal data, and the safety of network and information systems. Breaches are defined as acts or omissions that are unlawful and relate to the above-listed areas or that defeat the object or purpose of the rules in these areas (Art. 5 No. 1).

## 2. Special Case Professional Duty of Confidentiality

The special case of professional duty of confidentiality must be differentiated from the confidentiality duty of an employee pursuant to Art. 321a para. 4 CO. In respect of employees the CH-Draft-CO contains a reservation regarding professional secrecy (Art. 321 CH-StGB, Art. 47 CH-BankG[30], Art. 43 BEHG[31]) and exempts the employees from the

---

25 Each fact that is cumulatively known to a limited circle of persons and not publicly available, in respect of which the employer has a legitimate interest in maintaining confidentiality and in respect of which the employer has a will to maintain confidentiality which is, at least, apparent from the circumstances or probable; *Ullin Streiff & Adrian von Kaenel & Roger Rudolph,* Arbeitsvertrag, Praxiskommentar zu Art. 319–362 OR, 7. Aufl., Zürich 2012, Rn. 12 zu Art. 321a OR .

26 Additional Report (*Zusatzbotschaft*), BBl 2019 1409, 1414 et seq. and 1422.

27 Additional Report (*Zusatzbotschaft*), BBl 2019 1409, 1425.

28 See section. III. D.1.

29 Additional Report (*Zusatzbotschaft*), BBl 2019 1409, 1425.

30 Swiss Federal law on banks and saving banks as of 8 November 1934 (*Bundesgesetz vom 8. November 1934 über die Banken und Sparkassen, Bankengesetz, BankG*) SR 952.0.

31 Swiss Federal law on stock exchanges and securities trading as of 24 March 1995 (*Bundesgesetz vom 24. März 1995 über die Börsen und den Effektenhandel, Börsengesetz, BEHG*) SR 954.1.

new regulations (Art. 321a$^{septies}$ CH-Draft-CO). This concerns, next to medical confidentiality, inter alia, attorney-client privilege and banking secrecy. To the extent that no other legal justifications apply, professionally privileged persons reporting irregularities can rely only on the justifications of safeguarding justified interests.[32] In Art. 3 para. (3) the EU Whistleblower Protection Directive states that the Directive does not affect the protection of legal and medical professional privilege.

## D. Three-Step Reporting Cascade

The CH-Draft-CO provides for a three-step reporting cascade pursuant to which the whistleblower shall report, first, to the employer, then to the competent authority, and only in the last step to the public. Provided that employees comply with this cascade and its preconditions the report of an irregularity is basically deemed to comply with the fiduciary duty (Art. 321a$^{bis\,0}$ CH-Draft-CO). This reporting cascade codifies the rulings of the Swiss Federal Supreme Court on permitted whistleblowing in Switzerland.[33]

Also, employees do not violate their fiduciary duty if they obtain advice from a person subject to statutory confidentiality regarding their right to report irregularities (Art. 321a$^{sexies}$ CH-Draft-CO).

In detail, the conditions and requirements of each cascade remain complex for employers as well as employees in spite of the statutory basis.

### 1. Report to Employer (1st Cascade)

Employees must generally always report irregularities first to the employer (1st Cascade).

In this respect the CH-Draft-CO provides for a statutory assumption that a report to the employer has an effect if the employer creates an independent office for the receipt and handling of reports, draws up rules on the subsequent treatment thereof, prohibits terminations and other detriments due to a report, and allows for reports to be made anonymously (Art. 321a$^{quater}$ para. 2 CH-Draft-CO). Therewith, the legislator intends to set an incentive for the implementation of whistleblowing systems. If a whistleblowing system is introduced, the whistleblower must prove that the reporting procedures are ineffective and that a report to the employer would therefore have no impact.[34] Thus, in the case of an implemented reporting system, a report directly to the competent authority is possible only in exceptional circumstances.[35] The legislator does not explicitly state, however, that the lack of a whistleblowing system authorizes the whistleblower to report directly to the authorities. Even if a whistleblowing system is not in place, such reporting, pursuant to

32 BGE 6B_1369/2016, E.6. dated 20 July 2017.

33 BGE 127 III 310 dated 30 March 2001; BGE 4A-2/2008 dated 8 July 2008.

34 Additional Report (*Zusatzbotschaft*), BBl 2019 1409, 1417.

35 Additional Report (*Zusatzbotschaft*), BBl 2019 1409, 1427.

the wording of the draft law, is permitted only if the whistleblower may legitimately expect that a report (e.g. to the superior) will have no effect.

The EU Whistleblower Protection Directive, too, sets a preference and clarifies that the use of internal channels is preferred over external channels in cases where the breach can be addressed effectively internally (Art. 7 (2)).

### a) Internal Whistleblowing Systems

The employer is left with sufficient freedom in designing its whistleblowing system: Art. 321a$^{bis}$ CH-Draft-CO does not contain – contrary to the regulations pursuant to Art. 321a$^{quater}$ para. 2 CH-Draft-CO – any specifications on how to design an internal whistleblowing system. It must be suitable for the appropriate handling of reports and secure an independent handling of the report.[36]

#### aa) Permitted Reporting Channels

The CH-Draft-CO differentiates between *internal* and *external persons* and *offices* that are authorized to accept a report (Art. 321a$^{bis}$ para. 1 letter b. CH-Draft-CO). An authorized internal *person* may be the superior, the management, the board of directors (*Verwaltungsrat*) of a stock corporation,[37] or the compliance officer. As an internal *office* nominated by the employer and authorized to accept a report, the compliance department or the HR department may be considered in particular. Mostly, in Swiss practice, the management, the compliance department, and the HR department are responsible for accepting reports.[38]

Alternatively, the employer may delegate these roles and appoint an external representative. In that respect the employer may rely on its own solution (e.g. appointment of an attorney as ombudsperson) or on an industry solution, i.e., a solution offered by a third party to a specific business sector. In the latter case, associations for example could create an ombudsman's office for their sector for those members who for cost reasons cannot afford their own ombudsperson. This could be a solution, for example, for non-profit organizations such as charitable foundations or associations.[39]

If an employer has implemented a reporting office, the whistleblower is deemed to be acting in accordance with his or her fiduciary duty only if he or she delivers the report to such a reporting office (Art. 321a$^{bis}$ para. 1 letter b. CH-Draft-CO).

---

36 Additional Report (*Zusatzbotschaft*), BBl 2019 1409, 1417.

37 Additional Report (*Zusatzbotschaft*), BBl 2019 1409, 1416 and 1422.

38 Christian Hauser, Nadine Hergovits & Helene Blumer, *Whistleblowing Report 2019*, Chur 2019, 43.

39 Rita Pikó, *Compliance bei Non-Profit-Organisationen – Teil 2, Unter besonderer Berücksichtigung von gemeinnützigen Stiftungen und Vereinen in Deutschland und der Schweiz*, CB, 263, 264 et seq. (2018).

The EU Whistleblower Protection Directive follows the same understanding, pursuant to which reporting channels may be operated internally by appointed persons or offices or externally by a third party (Art. 8 (5)).

### bb) Plausible Suspicion

A further condition for the employee to comply with the fiduciary duty, next to reporting to a reporting office determined by the employer, is the existence of a plausible suspicion (Art. 321a[bis] para. 1 letter a. CH-Draft-CO). In the new version of the draft law the term *sufficient suspicion* ("*hinreichender Verdacht*") was replaced by *traceable suspicion* ("*nachvollziehbarer Verdacht*") to achieve a better cohesion between the French- and the Italian-language versions of the draft law.[40] Accordingly, at the time of reporting the whistleblower must have had objective reasons to assume an irregularity.

### cc) Reporting Channels

A decisive factor in the successful use of whistleblowing systems is positive communication and information for employees on the available reporting channels. The whistleblowing system will be used only if its existence is known of and trusted. It is left to the discretion of the employer to decide what channels are permitted for the reporting. Reports may be made through meetings in person, in writing (letter, fax, email), by phone or through special reporting channels such as mobile apps, social media, or Internet-based whistleblowing systems. In practice, Swiss companies offer three different reporting channels: email, meetings in person at the responsible office, and reporting by phone. Only 31% of the companies offer an Internet-based whistleblowing system.[41]

Pursuant to the EU Whistleblower Protection Directive, reports must be allowed in writing and/or orally as well as through meetings in person (Art. 9 (2)).

### dd) Anonymous Reporting

The EU Whistleblower Protection Directive leaves it to the respective Member State whether anonymous reports must be accepted and handled (Art, 6 (2)). The CH-Draft-CO permits *anonymous* reports[42] and therewith recognizes that anonymous reports may, under given circumstances, be the only means by which a whistleblower may report irregularities without risk.[43] Among the large corporations in Switzerland, 73% allow for anonymous reports. The need for such a solution is demonstrated by the fact that 58% of the

---

40 Additional Report (*Zusatzbotschaft*), BBl 2019 1409, 1422.

41 Christian Hauser, Nadine Hergovits & Helene Blumer, *Whistleblowing Report 2019*, Chur 2019, 36.

42 Art. 321a[quater] Para. 2 letter d. CH-Draft-CO.

43 The additional report mentions the internet-based whistleblowing system of the Swiss Federal Audit Office (*Eidgenössische Finanzkontrolle*) as an example (https://www.efk.admin.ch/de/whistleblowing-d.html) as

initial reports received by these corporations do not refer to the identity of the whistleblower.[44]

#### ee) Abuse of the Whistleblowing System

It is often feared that the implementation of whistleblowing systems – in particular, if anonymous reporting is permitted – increase abuse and bolster false accusations.[45] No statistical evidence, however, supports such a fear: one study shows that only 3% of all reports qualify as abusive. On the contrary, anonymous whistleblowers basically report in good faith.[46] Besides, the anonymous reporting has – contrary to the often-voiced concerns – no influence on the amount of abusive reports.[47]

The employer should clearly communicate its expectations when implementing a whistleblowing system, similar to the implementation of other compliance measures. Accordingly, a clear signal that the abuse of the whistleblowing system for one's own purposes or even defamation will trigger disciplinary sanctions is recommended. For this reason, Art. 23 (2) of the EU Whistleblower Protection Directive states that the Member States must provide for effective, appropriate and dissuasive penalties in respect of persons where it is established that they knowingly reported false information. In addition, measures for compensatory damages resulting from such false reporting must be provided for.

### b) Duty of Action for Employers

#### aa) Taking of Adequate Measures

The employer is obliged to follow up on a report, irrespective of whether the employer provides for an internal reporting system or not.[48] The CH-Draft-CO refers in this respect to the duty to take adequate (*genügende*) measures to handle the report (Art. 321a$^{bis}$ para. 2 letter c. CH-Draft-CO). Deliberately, it is not specified what is meant by the term "*genügend*".[49] Whether measures in the specific case are adequate shall be objectively reasoned and may not be judged from the subjective point of view of the employer or the whistleblower. Criteria for the judgement of the measures taken by the employer are, in

---

well as of the Federal Office of Police (*Bundesamtes für Polizei*) (https://www.bkms-system.ch/EFK-de www.whistleblowing.admin.ch); BBl 2019 1409, 1423.

44 Christian Hauser, Nadine Hergovits & Helene Blumer, *Whistleblowing Report 2019*, Chur 2019, 39/59.

45 SwissHoldings Sessionsticker (Sommerssession 2019) dated 29 May 2019, 2 (2 Mar. 2020) https://swissholdings.ch/wp-content/uploads/2019/05/Ticker-Sommersession-2019.pdf.

46 Christian Hauser & Lea Stühlinger, *Meldestellen für Hinweisgeber: Unternehmen und Politik sind gefordert*, CB, 447 (2018).

47 Christian Hauser, Nadine Hergovits & Helene Blumer, *Whistleblowing Report 2019*, Chur 2019, 10.

48 Additional Report (*Zusatzbotschaft*), BBl 2019 1409, 1427.

49 Additional Report (*Zusatzbotschaft*), BBl 2019 1409, 1419.

particular, the speed and appropriateness of the employer's reaction in respect of the reported irregularity.[50]

An example for a sufficient measure for handling a report is an initial, preliminary examination of the merits, followed by a triage. The office carrying out the examination must decide whether the case should be investigated and, in particular, whether the investigation should be conducted internally or with external support. Corporates should standardize these processes in an early stage, to be able to conduct, upon receipt of a report, the processes in an efficient, speedy and effective way. According to one study, only 50% of the questioned corporations actually follow this advice.[51]

The employer can determine the subsequent measures only after the incident has been investigated and resolved. By regularly informing the whistleblower on the status of the investigation and how it is being handled, the employer can signal to the whistleblower that the report is being taken seriously and is being investigated. This shall strengthen trust both in the employer and in the whistleblowing system.

### bb) Deadlines for Handling the Report

The CH-Draft-CO imposes duties on the employer to act on a received report. Under the draft, the employer must establish an appropriate deadline of no more than 90 days from receipt of a report for its handling (Art. 321a$^{bis}$ para. 2 letter a CH-Draft-CO). The CH-Draft-CO thereby aims to address different possibilities: simple and urgent cases that require a quick response and a correspondingly shorter deadline, and more complex cases that may require a longer investigation.[52] It seems that the Swiss legislator intended to oblige the employer to conclude an investigation of a report on irregularities within no more than 90 days. For complex matters, however, practice shows that this deadline cannot be met. Certain internationally known compliance cases that have been investigated internally have taken several years to conclude. A different, more practically orientated interpretation of this draft provision would be that the employer is obliged to start investigation measures within the deadline of 90 days but need not, by law, have concluded them within that time.

The employer is obliged to inform the whistleblower on the receipt and the handling of the report (Art. 321a$^{bis}$ para. 2 letter b. CH-Draft-CO) independently of whether a whistleblowing system has been implemented or not.[53] The employer is exempt from this obligation only if the report is anonymous, which makes the obligation impossible or apparently unreasonable for the employer to fulfil. The CH-Draft-CO does not state at what

50 Additional Report (*Zusatzbotschaft*), BBl 2019 1409, 1424.

51 Christian Hauser & Lea Stühlinger, *Meldestellen für Hinweisgeber: Unternehmen und Politik sind gefordert*, CB, 446 (2018).

52 Additional Report (*Zusatzbotschaft*), BBl 2019 1409, 1424.

53 Additional Report (*Zusatzbotschaft*), BBl 2019 1409, 1427.

point in time the employer must inform the whistleblower on the handling of a report (Art. 321a$^{bis}$ para. 2 letter b. CH-Draft-CO).

The EU Whistleblower Protection Directive is more concrete in these aspects: the employer must confirm receipt of a report within seven days to the whistleblower (Art. 9 (1) letter b). Within three months of that confirmation the employer is obliged to inform the whistleblower on the subsequent measures taken (Art. 9 (1) letter f). Such subsequent measures include actions to assess the accuracy of the allegations made in the report and to stop the reported violation (Art. 5 No. 12).

## 2. Report to Authorities (2nd Cascade)

If an employer does not comply with its statutory duties upon receipt of a report on irregularities (see above section D.1.b.) the whistleblower is entitled to inform the competent authorities on the irregularities without violating his or her fiduciary duty (Art. 321a$^{ter}$ CH-Draft-CO). The same applies if, due to his or her report to the employer, the whistleblower's employment contract is terminated or the whistleblower experiences other detrimental consequences (Art. 321a$^{ter}$ letter b. CH-Draft-CO).

A whistleblower may signal a report directly to an authority, i.e. without a previous report to the employer, if there exists plausible suspicion and the whistleblower may assume that (i) a report to the employer will have no effect, or (ii) the competent authority would be prevented in its duties without an immediate report to it, or (iii) there exists an immediate and severe threat to lives, health or the safety of persons or the environment or an immediate danger of great damage. (Art. 321a$^{quater}$ CH-Draft-CO). Whether, in a given situation, a danger exists or merely threatens is based on the assessment by the whistleblower.[54]

The authority competent to verify compliance with the violated regulation is the recipient of a report on irregularities: the prosecution authorities in the case of criminal acts, and the administrative authorities in the case of a violation of public law. The CH-Draft-CO specifies that, to be able to report to authorities, the irregularities must concern regulations subject to control by an authority. This basically excludes irregularities in civil law that concern, exclusively, a legal relationship between private persons. Irregularities may, however, be reported to authorities in spite of their association with civil law where the legal relationship is between a private person and an authority and is covered, for example, by the law on the protection of adults (*Erwachsenenschutzrecht*) or company registration law.[55]

Accordingly, additional violations determined by the employer that do not qualify as a violation of law verifiable by authorities cannot be reported to an authority. Rather, the employee would in such a case probably be in breach of his or her fiduciary duty. Any

54 Additional Report (*Zusatzbotschaft*), BBl 2019 1409, 1428.

55 Additional Report (*Zusatzbotschaft*), BBl 2019 1409, 1426.

informing of the public in a case that does not breach fiduciary duty is not intended by the CH-Draft-CO either, as such a report mandatorily requires, first, a report to the competent authority (Art. 321a$^{quinquies}$ CH-Draft-CO, see below section III.D.3.).

In this context it should be further noted that the regulations apply only to reports to domestic and not to foreign authorities.[56] A report to a German authority of a criminal irregularity by an employee of a Swiss subsidiary of a German company, for example, would therefore not be protected by the CH-Draft-CO.

Pursuant to Art. 10 of the EU Whistleblower Protection Directive, employees may report to authorities after having made use of internal channels. Alternatively, subject to certain conditions, they may report directly to the competent authority.

### 3. Disclosure to the Public (3rd Cascade)

Pursuant to the CH-Draft-CO, disclosure to the public by a whistleblower is an exception. The whistleblower that discloses irregularities to the public is deemed to comply with his or her fiduciary duty only if (i) the whistleblower reported the irregularity to the competent authority and received no appropriate response within 14 days thereafter, or (ii) the whistleblower's employment contract was terminated following the report to the authority, or (iii) the whistleblower experienced other detrimental consequences (Art. 321a$^{quinquies}$ letter c. CH-Draft-CO). A further condition is that the whistleblower has serious reasons to believe – in good faith – that the reported circumstances are true (Art. 321a$^{quinquies}$ letter a. CH-Draft-CO). By these conditions the legislator increases the hurdle compared to the preceding steps of cascades that require only that a whistleblower has a plausible suspicion.[57] Under Art. 14 CH-StGB, the whistleblower is deemed to be acting justly only if all these conditions are met.[58]

In the final version of the EU Whistleblower Protection Directive the conditions for protection of a whistleblower if he or she discloses information to the public was redefined (Art. 15). Accordingly, a whistleblower must (i) initially report to an internal or external reporting channel or directly externally if no appropriate action was taken in response to the report within the relevant timeframe, and (ii) the whistleblower has reasonable grounds to believe that (iii) the violation may constitute an imminent or manifest danger to the public interest or, in the case of external reporting, there is a risk of retaliation or there is low prospect of the violation being effectively addressed.

56 Additional Report (*Zusatzbotschaft*), BBl 2019 1409, 1417.

57 Additional Report (*Zusatzbotschaft*), BBl 2019 1409, 1417.

58 Additional Report (*Zusatzbotschaft*), BBl 2019 1409, 1414.

| | | | |
|---|---|---|---|
| **3rd Cascade (Public)** | **Disclosure to the Public** | | |
| | complies with the employee's fiduciary duties, if<br>• employee has **serious reasons** to consider the reported circumstances to be true<br>• **after reporting to the competent authority** AND<br>• competent authority did not inform employee on the handling of the report **within 14 days** despite request OR<br>• employee was **laid-off** after the report to the authority or has experienced other detrimental consequences | | |
| **2nd Cascade (Authority)** | **Report to Competent Authority without prior report to employer** | **Report to Competent Authority following report to employer** | **Compulsory Measures by Authority** |
| | is compliant with employee's fiduciary duty, if<br>• employee has **plausible suspicion** of an irregularity AND<br>• employee **did not previously** report to employer AND<br>• employee reasonably deems that report to employer **will not have any effect** OR<br>• competent authority would **be prevented** in its duties without immediate report to it OR<br>• there is an **immediate** and **severe threat** to lives, health or the safety of persons or the environment or an immediate danger of great damage | is compliant with employee's fiduciary duty, if<br>• employee has **plausible suspicion** of an irregularity AND<br>• employee **did previously** report to employer first AND<br>• employer **did not take compulsory measures within 90 days** OR<br>• employee was **laid-off** after the report or has experienced other **detrimental consequences** | • competent authority must inform employee on the handling of the report **within 14 days** |
| **1st Cascade (Employer)** | **Report to Employer** | **Report to Employer** | **Compulsory Measures by Employer** |
| | is compliant with employee's fiduciary duty, if<br>• employee has **plausible suspicion** of an<br>• **irregularity** =<br>- breach of **law**<br>- breach of **internal regulations**<br>• **no** reporting office exists | is compliant with employee's fiduciary duty, if<br>• employee has **plausible suspicion** of an<br>• **irregularity** =<br>- breach of **law**<br>- breach of **internal regulations**<br>• reported to **reporting office** | • duty to handle report **within 90 days**<br>• **confirmation of receipt** of report + treatment steps<br>• initiation of **sufficient measures** |

© Chart by Dr. Rita Pikó

| Whistleblower | | |
|---|---|---|
| • employee in the **private** sector<br>• **right to report**<br>• **anonymous** reports are permitted<br>• employee may take advice from a person subject to statutory confidentiality duty | | |
| **Regulatory Approach** | **Protection of Employer from reports to Third Parties** | **Protection of Employee** |
| • **no statutory or self-regulatory duty** to implement a reporting system.<br>• however, legal **incentive** to implement an internal reporting system to prevent reporting to authority or public | protection of employer from reports by employee to authority or public through **statutory assumption** that a report has an effect, if employer<br>• provides for an independent office for the receipt and handling of reports<br>• provides for regulations for the handling of reports (whistleblowing procedures)<br>• prohibits dismissals and other detrimental consequences<br>• allows for anonymous reports | • termination of employment contract by employer is abusive if employee reports in compliance with fiduciary duty<br>• employer is obliged to ensure that employer incurs no detrimental consequences due to submitting a report |

© Chart by Dr. Rita Pikó

## E. Employer's Duties Regarding the Protection of the Whistleblower

The employer must ensure that the whistleblower incurs no disadvantages when reporting in compliance with the above described order of cascade. Further, the whistleblower may incur no disadvantages from consulting on the reporting rights with a person subject to statutory secrecy obligations (Art. 328 para. 3 CH-Draft-CO). The legislator does not define the meaning of disadvantages, nor what protection measures must be implemented by the employer, nor what consequences are triggered by a breach of such duties.

The EU Whistleblower Protection Directive explicitly specifies in Art. 19 what actions qualify as retaliation and obliges the member states to take measures to prohibit any form of retaliation. Such retaliations include, inter alia, suspension, lay-off, demotion or withholding of promotion, reduction in wages, negative performance assessment, intimidation, discrimination, harm to the person's reputation, including the threat and attempt of these retaliations. In addition, extensive safeguards are provided: whistleblowers shall not incur any liability for breach of contractual or statutory restrictions on disclosure of information (Art. 21). Whistleblowers are entitled to fair proceedings and the right to be

heard, effective remedy and right to access their file (Art. 22). Persons that hinder or try to hinder reports, retaliate or breach the duty of maintaining confidentiality duties are subject to penalties (Art. 23 (1)).

## F. Abusive Lay-Off

Swiss employment law is marked by the principle of freedom to terminate an employment contract. Employers and employees may ordinarily terminate an unlimited employment relationship without objective justification, subject to notice periods and termination dates pursuant to Art. 334 et seq. CO, respectively without notice pursuant to Art. 337 et seq. CO.

Art. 336 CO provides for an objective protection from termination by an exemplary listing of abusive circumstances. The draft law intends to extend these abusive circumstances to include the termination of the employment relationship by the employer due to the whistleblower reporting an irregularity in compliance with the cascade or due to the whistleblower taking advice in that respect (Art. 336 para. 2 letter d. CH-Draft-CO). In this case the whistleblower may, in accordance with Art. 336b (1) CO, raise an objection with the employer against the termination until the end of the period of notice.

The labor law consequences of an abusive termination are laid down in Art. 336a CO, respectively Art. 337c CO. In the case of an abusive ordinary termination the whistleblower is entitled to compensation of up to the equivalent of six months' salary. In the case of an abusive termination without notice the whistleblower is entitled, pursuant to Art. 337c CO, to what he or she would have earned had the employment relationship been terminated in compliance with the ordinary notice period.

The termination, however, remains effective. The Swiss Federal Council (*Bundesrat*) deliberately wishes to go no further.[59] The CH-Draft-CO does not provide for grandfathering of the whistleblower or an explicit prohibition of retaliation or even a penalty for abusive termination. Rather, the legislator relies on the deterrent effect of a whistleblower informing the public should the whistleblower be laid off or incur other detrimental consequences, and provided that the other conditions are satisfied.[60]

---

59 Report of the partial revision of the Swiss Code of Obligations (*Botschaft über die Teilrevision des Obligationenrechts*) dated 20 November 2013, BBl 2013 9513, 9515: "An abusive or unjustified notice following a report which does not violate the fiduciary duty will continue to be sanctioned in accordance with applicable law. (...) An additional protection against notice just for the case of a report of an irregularities cannot be justified compared to other reasons for an abusive notice." („*Eine missbräuchliche oder ungerechtfertigte Kündigung im Anschluss an eine Meldung, die nicht gegen die Treuepflicht verstösst, wird weiterhin nach dem geltenden Recht sanktioniert. (...) Ein erweiterter Kündigungsschutz nur für den Fall der Meldung einer Unregelmässigkeit lässt sich im Vergleich mit anderen Gründen für eine missbräuchliche Kündigung nicht rechtfertigen.*").

60 It is noteworthy that the whistleblower may notify the public only if the employer gave notice to the whistleblower or the whistleblower incurred other detrimental consequences after his or her report to the authorities.

## IV. OUTLOOK

Statutory regulation of the conditions for permissible whistleblowing in Switzerland is undoubtedly necessary to provide legal certainty for whistleblowers and employers. The Legal Affairs Committee of the Swiss National Council (*Nationalrat*) dismissed the draft of the Swiss Federal Council (*Bundesrat*) on "Whistleblowing", reasoning that following its revision the draft of the Swiss Federal Council (*Bundesrat*) still remains very complex and hard to understand for employees.[61] The Swiss National Council (*Nationalrat*) "neatly" buried the draft law the first time on 3 June 2019, and for the second time and definitely on 5 March 2020.[62] At the end of the debate of the Swiss National Council (*Nationalrat*) the Swiss Federal Councillor (*Bundesrätin*), Karin Keller-Sutter stated that she cannot promise a different or better submission; in effect, that the Swiss Federal Council (*Bundesrat*) will not be able to take action nor will it be able to present a new submission immediately.[63]

In the end, following a long legislative process, whistleblowers in Switzerland remain without statutory protection. Swiss corporations with foreign business must deal with foreign rules, i.e. the EU Whistleblower Protection Directive, on their own. Presumably, the OECD's evaluation of Switzerland may not become a positive evaluation in the short term.

Pursuant to the draft act, the whistleblower may not lawfully inform the public if (i) the whistleblower fruitlessly reported to the employer and the employer thereupon gave notice to the whistleblower (ii) the whistleblower thereupon fruitlessly informed the authorities, and the other conditions for the lawful information of the public are met. For Art. 321a$^{quinquies}$ letter c. nº 2 CH-Draft-CO states that the public may be informed only if the whistleblower was given notice after his or her report to the authority – but not before.

61 On 3 May 2019 the Legal Affairs Committee of the Swiss National Council dismissed the proposal of the Swiss Federal Council on "Whistleblowing" by 19 to 4 votes; press release of the Legal Affairs Committee of the Swiss National Council dated 3 May 2019, (13 Mar. 2020) https://www.parlament.ch/press-releases/Pages/mm-rk-n-2019-05-03.aspx.

62 Swiss National Council in favor of a "neat burial" of the whistleblowing proposal, notice dated 13 May 2020; https://www.parlament.ch/de/services/news/Seiten/2019/20190603185414556194158159041_bsd155.aspx.

63 Speech of Federal Councilor Karin Keller-Sutter, (13 Mar. 2020) https://www.parlament.ch/de/ratsbetrieb/amtliches-bulletin/amtliches-bulletin-die-verhandlungen?SubjectId=48524#votum12.

CEJ
COMPLIANCE
ELLIANCE
JOURNAL

# WILL DIGITAL CURRENCIES REPLACE CASH? – DIGITAL CURRENCY, PRIVACY, AND SURVEILLANCE

Fabian Teichmann & Marie-Christin Falker

## AUTHORS

*Fabian M. Teichmann is an attorney-at-law and public notary in Switzerland. After earning an undergraduate degree in economics and finance (Bocconi University, Italy), he then earned graduate degrees in management (Harvard University, USA), accounting and finance, and law (University of St. Gallen, Switzerland). He also holds a PhD in law (University of Zurich, Switzerland), a doctoral degree in economics and social sciences (Kassel University, Germany), and an LL.M. (King's College, UK). Teichmann teaches courses on compliance, corruption, money laundering, and terrorism financing at various universities. He is the author of several books and over 100 scholarly articles.*

*Marie-Christin Falker is a research associate at Teichmann International (Schweiz) AG. She possesses an undergraduate degree in English and American Culture and Business Studies, focusing particularly on international management and marketing (Kassel University, Germany). She also studied at the University of Maryland, College Park (USA) as an undergraduate.*

## ABSTRACT

*In some nations, including Sweden and South Korea, cash payments are becoming increasingly uncommon. Other nations, such as Germany, continue to predominantly prefer cash. At the same time, digital currency is on the rise, and the announced launch of Facebook's stablecoin Libra, in particular, has caused a debate around digital money. In response, a number of central banks have begun to consider launching their own versions of digital currency. This article analyzes characteristics of both cash and digital currency and illustrates advantages as well as disadvantages of digital money and a cashless society. In particular, privacy concerns regarding digital cash are addressed. In addition, compliance risks are highlighted, and it is deliberated whether the introduction of digital cash could lead to a decrease in crime related to cash and cryptocurrencies.*

## TABLE OF CONTENTS

## I. INTRODUCTION

The race for a central bank-issued digital currency has begun. Research conducted by cryptocurrency and blockchain research and analysis group The Block analyzed 60+ central banks and found that 18 of these banks publicly acknowledged they were developing a digital currency. These include the central banks of China, Singapore, Iran, UAE, and Europe. Four countries, namely, Tunisia, Senegal, Venezuela, and Uruguay, have already launched their versions, whereas the others have launched pilots or are still in development[1]. In particular, the announced launch of Facebook's Libra cryptocurrency is currently motivating central banks to come up with digital equivalents of their governmental currencies[2]. China seems to be particularly eager to replace cash with a digital currency[3].

At the same time, the public is becoming increasingly aware of government surveillance techniques and the resulting lack of privacy. Nations such as China are suspected of taking government surveillance to extremes. In China, technologies such as facial recognition are being used to monitor citizens in nearly every aspect of their lives, including crossing the street (which could result in a jaywalking fine) and purchasing a sim-card for a mobile phone (new purchases require users to scan their face). In the context of this extensive governmental surveillance, which is mainly performed using new technology, China's announcement of the intention to introduce a digital currency has caused a debate on whether the Chinese government could attempt to use the currency to monitor its citizens. Because of the possibility of such behavior by governments, many citizens in China and elsewhere are likely to be opposed to the introduction of central bank-issued digital currencies. After all, recent changes brought about by digitalization, which include data brokers' selling of personal data to advertisers and the Cambridge Analytica scandal, where the company used personal data of up to 87 million Facebook users to facilitate Donald Trump's political campaign[4], are causing privacy to become an increasingly valuable good. Kenneth Rogoff, former International Monetary Fund chief economist, admits in his book *The Curse of Cash*, "We need cash for privacy"[5].

---

1 S. Zheng, *At Least 18 Central Banks are Developing Sovereign Digital Currencies*, THE BLOCK (Dec. 26, 2019, 1:45 PM EST), https://www.theblockcrypto.com/linked/51526/at-least-18-central-banks-are-developing-sovereign-digital-currencies?utm_source=newsletter&utm_medium=email&utm_campaign=2019-12-26.

2 M. Orcutt, *An Elegy For Cash: The Technology We Might Never Replace*, MIT TECHNOLOGY REVIEW (Jan. 3, 2020), https://www.technologyreview.com/s/614998/an-elegy-for-cash-the-technology-we-might-never-replace/?utm_source=newsletters&utm_medium=email&utm_campaign=+the_download.unpaid.engagement.

3 R. Zhong, *China's Cryptocurrency Plan Has a Powerful Partner: Big Brother*, THE NEW YORK TIMES (Oct. 18, 2019), https://www.nytimes.com/2019/10/18/technology/china-cryptocurrency-facebook-libra.html.

4 Tagesanzeiger, *Facebook wegen Cambridge Analytica angeklagt* (Dec. 19, 2018), https://www.tagesanzeiger.ch/ausland/amerika/facebook-wegen-cambridge-analytica-angeklagt/story/31385518 .

5 Rogoff quoted in J. Pethokoukis, *The Problem with Cash: A Q&A with Economist Kenneth Rogoff*, AMERICAN ENTERPRISE INSTITUTE (Nov. 10, 2016), https://www.aei.org/economics/the-problem-with-cash-a-qa-witheconomist-kenneth-rogoff/.

## II. CHARACTERISTICS OF CASH

The term "cash" refers to money in the forms of coins and bills. These are bearer instruments, which means that whoever holds them is assumed to be their owner. Cash transactions are peer-to-peer; there is no third party, such as an intermediary, involved and ownership can be transferred simply by handing over the cash[6]. There is not necessarily even a record of the transaction. Therefore, cash is considered to be highly anonymous. If records are not made, transactions using cash cannot easily be reconstructed. Further, contrary to digital payments, cash provides no data that could be used by companies to build advertising profiles or credit ratings. Similarly, cash does not facilitate governmental tracking of spending and individuals[7]. Moreover, hardly any trust is required in cash transactions: as long as one can verify its legitimacy, there is no danger of losing the money, as would be the case, for instance, if one accepted a check from an insolvent bank[8].

Further, cash is permissionless, which means it does not require authorization from an institution in order to be used in a transaction. In contrast, people who do not have good credit, a government ID, steady income, or a permanent address will have difficulty opening a bank account. Gender discrimination could also be an issue: some countries do not allow women to open bank accounts[9]. With cash, every person can participate in the system without first being granted permission[10]. The permissionlessness of cash also makes it resistant to censorship, which means it can be used for illegal or culturally taboo activities[11]. As a result, payment by cash is a preferred modus operandi for a wide variety of criminals, including drug dealers, arms dealers, and many others.[12]

Because cash is used in the majority of transactions related to organized crime, money laundering (as a necessary consequence of such use) has become a significant threat to national economies and is a global problem[13]. Its effects are felt on a microeconomic scale in the private sector, within which money launderers use front companies to mix legitimate and illegitimate income. In some cases, front companies even sell products at prices below manufacturing cost, which gives them an advantage over legitimate businesses[14].

---

6 J. Brito, *The Case for Electronic Cash: Why Private Peer-to-Peer Payments are Essential to an Open Society*, COIN CENTER (Feb., 2019), https://coincenter.org/files/2019-02/the-case-for-electronic-cash-coin-center.pdf.

7 Orcutt, *supra* note 2.

8 Brito, *supra* note 6.

9 M. Coker, *How Guardianship Laws Still Control Saudi Women*, THE NEW YORK TIMES (June 22, 2018), https://www.nytimes.com/2018/06/22/world/middleeast/saudi-women-guardianship.html.

10 Brito, *supra* note 6.

11 Brito, *supra* note 6.

12 F. TEICHMANN, UMGEHUNGSMÖGLICHKEITEN DER GELDWÄSCHEREIPRÄVENTIONSMASSNAHMEN [in German] 3 (Schulthess) (2016).

13 J. Harvey, *An evaluation of money laundering policies*, 8 J MON L CONT 339 (2005).

14 This could be the case with real estate, see e.g., F. Teichmann, *supra* note 12 at 155.

This can lead to the crowding out of private sector businesses by criminal organizations. Ultimately, these organizations' management principles do not concur with traditional free market principles, which leads to negative microeconomic and macroeconomic effects[15]. Money laundering laws have been widely established to facilitate the conviction of criminals, particularly those involved in the drug trade. However, for a variety of reasons, money laundering continues to pose a threat to the public[16].

Money launderers frequently operate within networks of cooperation with other criminals. Therefore, their laundering methods are extremely difficult to substantiate[17]. When working with banks, money launderers utilize front people in order to remain anonymous. These front people pose as the beneficial owners of front companies and bank accounts[18]. Some jurisdictions, such as Dubai, are more cash-intensive than others and so tend to be preferred by money launderers[19]. In addition, the increasing density of compliance and know-your-customer (KYC) regulations in the financial sector has caused many money launderers to relocate their activities to less regulated sectors[20]. These include, among many others, the cryptocurrencies sector[21]. Bitcoin and other cryptocurrencies attempt to mimic the characteristics of cash; however, they are difficult to use and processing a transaction can be a slow process. Additionally, their values often fluctuate[22]. As a result, cash continues to be the most feasible option for individuals who either have no access to a bank account or wish to keep their transactions private.

## III. CHARACTERISTICS OF DIGITAL CURRENCY

"Digital Currency" is a blanket term that includes all forms of electronic money. Thus, virtual currencies and cryptocurrencies are (overlapping) types of digital currency. Digital currencies can be regulated or unregulated but are always intangible. Digital currencies that are spent using electronic wallets or networks are often called digital money. There are no intermediaries involved, which means transactions are fast and transaction fees are

15 J. McDowell, *The Consequences of Money Laundering and Financial Crime*, HOMELAND SECURITY DIGITAL LIBRARY (May, 2001), https://www.hsdl.org/?view&did=3549.

16 F.C. Razzano, *American Money Laundering Statutes: The Case for a Worldwide System of Banking Compliance Programs*, 3 J INT L & PRAC 277, (1994).

17 F. Teichmann & M.C. Falker, *Money Laundering – Currency Exchange*, J FIN REG COMP (forthcoming).

18 F. Teichmann & M.C. Falker, *Money Laundering Through Banks in Dubai*, J FIN REGULATION COMP (forthcoming).

19 F. Teichmann & M.C. Falker, *Money Laundering – The Gold Method*, J MON L CONT (forthcoming).

20 Teichmann, *supra* note 12 at 27.

21 F. Teichmann & M.C. Falker, *Money Laundering Through Cryptocurrencies, in*: Artificial Intelligence: Anthropogenic Nature vs. Social Origin (B.S. Sergi & E.G. Popkova eds, Springer, forthcoming).

22 Orcutt, *supra* note 2.

low[23]. Virtual currencies are a subset of digital currencies that are characterized as usually controlled by their creators and "accepted among the members of a specific virtual community"[24]. Virtual currencies represent a monetary value that is issued, managed, and controlled by private issuers and are used for peer-to-peer transactions. They can be represented by tokens and are not necessarily backed by legal tender. Owing to their lack of regulation, the prices of virtual currencies are rather volatile. Cryptocurrencies such as ethereum or Bitcoin are considered virtual currencies[25].

Cryptocurrencies are made secure by encryption algorithms and cryptographic techniques. For this reason, they are difficult to counterfeit. They often operate in systems that are blockchain-based and decentralized. These characteristics make the role of a trusted third party such as a central bank redundant. Instead, users transfer funds peer-to-peer with the use of private and public keys[26]. Bitcoin is the most well-known cryptocurrency. Cryptocurrencies share some characteristics with cash; in particular, they are highly anonymous. However, unlike cash, they are not completely anonymous, because details of every transaction (including users' public keys, the time, and the date) are recorded irrevocably on the blockchain. Like cash, cryptocurrencies have a reputation for being used for criminal activity, primarily owing to the fact that they are not controlled by a central entity and governments have very little jurisdiction over them. According to Jill Carlson, co-founder of Open Money Initiative, cryptocurrencies were not designed to solve mainstream issues such as speed of transactions and stable values; they were created to resist censorship. As a result, cryptocurrencies have been documented as being used to purchase drugs online, buy US dollars in Argentina, pay sex workers, make international monetary transfers, support dissidents in Hong Kong, and move money out of Venezuela[27]. Carlson furthermore argues: "It is time to face this potentially uncomfortable reality: cryptocurrency is most useful when breaking laws and social constructs"[28]. In conclusion, cryptocurrencies facilitate financial activities that would otherwise be prohibited or suppressed.

Like cash, privacy-preserving decentralized technologies have given organizations and people the opportunity to escape censorship. Although the actors in these domains act in accordance with certain regulations, government policies and social norms can hardly be enforced in these contexts. Therefore, stopping censored activities becomes much more

---

23 Y.B. Perez, *The Differences Between Cryptocurrencies, Virtual, and Digital Currencies*, THE NEXT WEB (Feb. 19, 2019, 9:14 UTC), https://thenextweb.com/hardfork/2019/02/19/the-differences-between-cryptocurrencies-virtual-and-digital-currencies/.

24 Id.

25 Id.

26 Id.

27 J. Carlson, *Cryptocurrency is Most Useful for Breaking Laws and Social Constructs*, COINDESK (Dec. 10, 2019), https://www.coindesk.com/cryptocurrency-is-most-useful-for-breaking-laws-and-social-constructs.

28 Id.

difficult[29]. Data collected by blockchain analytics company Chainalysis supports this claim: in 2019, $US2.8 billion in Bitcoin were transferred through crypto exchanges by criminals[30]. According to Chainalysis, crypto exchanges have always been "popular off-ramp for illicit cryptocurrencies"[31]. In addition, the share of illicit cryptocurrency has steadily grown since the beginning of 2019. Within the scope of their analysis, especially in relation to crypto exchanges, Binance and Huobi came under scrutiny. Although both exchanges have KYC protocols in place, the requirements are less stringent for over-the-counter (OTC) brokers. As a result, some OTC desks seem to have specialized in providing money-laundering services to criminals[32].

The small amount of quantitative data available also suggests that the use of cryptocurrency is more predominant in countries with financial restrictions[33]. Data on the cryptocurrency trade in Venezuela has shown that, between the petro (the central bank-issued digital currency) and decentralized cryptocurrency, citizens seem to prefer the latter. Experts also claim that in Palestine, where many financial services such as PayPal are not available, the awareness of Bitcoin and ethereum has increased since 2018. This is not only true for terrorism financiers, but also for irreproachable residents and businesspeople[34]. Thus, it can be assumed that in regions where the public distrusts the government or local currency, where hyperinflation is prevalent, or where there are simply no other alternatives available, residents frequently turn to cryptocurrency. Laws are not always considered acceptable by either citizens of the jurisdiction or by outsiders. Therefore, experts argue that it cannot be concluded that privacy-enhancing technologies are used primarily for illegal or socially unacceptable activities[35]. In particular, in societies and nations where government surveillance seems ubiquitous, citizens use both cash and cryptocurrencies or other privacy-enhancing technologies to protect their privacy.

29 Id.

30 Chainalysis Team, *Money Laundering in Cryptocurrency: How Criminals Moved Billions in 2019*, CHAINALYSIS INC (Jan. 15, 2020), https://blog.chainalysis.com/reports/money-laundering-cryptocurrency-2019.

31 Id.

32 Id.

33 M. Ahlborg, *Nuanced Analysis of LocalBitcoins Data Suggests Bitcoin is Working as Satoshi Intended*, MEDIUM (Feb. 8, 2019), https://medium.com/@mattahlborg/nuanced-analysis-of-localbitcoins-data-suggests-bitcoin-is-working-as-satoshi-intended-d8b04d3ac7b2.

34 L. Cuen, *In Palestine, Civilians Are Using Bitcoin More Than Hamas*, COINDESK (Aug. 22, 2019), https://www.coindesk.com/palestinian-civilians-are-using-bitcoin-more-than-terrorists.

35 Carlson, *supra* note 27.

# IV. LEGAL FRAMEWORK

## A. Data Protection

Data protection is perhaps the most pressing concern of citizens when it comes to digital currency or cash. In the following sections, we will present the legal framework for various jurisdictions of interest here.

### 1. China

China has no single comprehensive data protection laws. Instead, there are rules relating to data security and personal data protection that are part of a complex framework. These rules are incorporated across various regulations and laws. The General Principles of Civil Law and the Tort Liability Law have been used to interpret data protection as a right to privacy or right to reputation. These interpretations are, however, not explicit[36]. On June 1, 2017, the PRC Cybersecurity Law, which addresses data privacy protection and cybersecurity, came into effect. Under this law, the data protection obligations include, among others, guidelines on personal information and data security. Current data protection rules are based mainly on the Decision on Strengthening Online Information Protection, effective from December 28, 2012; the National Standard of Information Security Technology, a guideline that came into effect on February 1, 2013; and the National Standard of Information Security Technology, a Personal Information Security Specification that became effective on May 1, 2018[37]. Depending on the industry, provisions contained in other laws and regulations might also apply (e.g., for financial institutions, e-commerce businesses, and certain healthcare providers). Furthermore, provincial-level laws may need to be considered[38].

### 2. United States

In the United States, data security laws are largely sector-specific or medium-specific, and include laws and regulations that apply to financial institutions, personal health information, telecommunications firms, credit card information telemarketing, direct marketing, and children's information[39]. Among its 50 states and territories, the United States has an abundance of privacy and data security measures that consist of (but are not limited to) safeguarding data, privacy policies, disposal of data, and data breach notification. Further, the US Federal Trade Commission (FTC) has jurisdiction over many commercial entities under its authority in order to safeguard consumers from unfair trade or deceptive

---

36 DLA Piper, *Data Protection Laws of the World: China*, DLA PIPER (Last modified Dec. 31, 2019), https://www.dlapiperdataprotection.com/index.html?c=CN&c2=DE&go-button=GO&t=law.

37 Id.

38 Id.

39 DLA Piper, *Data Protection Laws of the World: USA*, DLA PIPER (Last modified Jan. 27, 2020), https://www.dlapiperdataprotection.com/index.html?t=law&c=US.

practices. The FTC issues regulations that enforce privacy laws and investigate firms for failing to implement reasonable data protection measures, failing to abide by applicable industry self-regulatory principles, and more. In addition, many state attorneys general have similar authority over unfair business practices[40].

### 3. European Union

In the European Union, the General Data Protection Regulation[41] (GDPR) entered into force in 2016. It became directly applicable in all member states on May 25, 2018 without requiring implementation through national law. An EU directive applies consistently across all member states and is directly applicable. Over 50 areas are covered by the GDPR; however, some are "permitted to legislate differently in their own domestic data protection laws"[42]. Any organization that processes personal data of data subjects in the European Union is obligated to abide by GDPR, even if it is not established within the EU. This concerns the offering of goods and services[43] and the monitoring of the organization's behavior[44]. In comparison with other regions, the EU regulates data privacy heavily.

### 4. Venezuela

Venezuela does not have general legislation that regulates data protection; instead, there are general principles established in the Constitution and developed by Supreme Court decisions[45]. The framework for personal data protection is based on principles established in the Constitution. The purpose of these principles is to safeguard the intimacy, private life, self-image, honor, confidentiality, and reputation of citizens. In addition, the Constitution establishes the right to access information and data: based on Article 28 of the Constitution, every person has the right to access information and data concerning themselves that is stored in public or private registries. They also have the right to be informed of how this information is used, and the right to rectify, update, and destroy incorrect information that unlawfully affects their rights. Information on individuals and their purchases may be collected, maintained, and arranged into profiles; this also includes their activities. These profiles must be intended for the benefit of the collecting entity or third parties, provided all constitutional rights are respected. Collectors of such information must also guarantee a number of principles, including the principle of free will, principle

---

40 Id.

41 General Data Protection Regulation, 2016/679 (EU).

42 DLA Piper, *Data Protection Laws of the World: Germany*, DLA PIPER (Last modified Jan. 14, 2020), https://www.dlapiperdataprotection.com/index.html?c=CN&c2=DE&go-button=GO&t=law.

43 General Data Protection Regulation, 2016/679, Art. 3 (2) (a) (EU).

44 General Data Protection Regulation, 2016/679, Art. 3 (2) (b) (EU).

45 DLA Piper, *Data Protection Laws of the World: Venezuela*, DLA PIPER (Last modified Jan. 28, 2019), https://www.dlapiperdataprotection.com/index.html?t=law&c=VE.

of confidentiality, and principle of responsibility. In addition, there is a law against cybercrime and the Banking Institutions Law, which regulates data protection in the sector[46].

## B. Cryptocurrencies

Because digital currency raises so many privacy concerns in relation to the wider public, it seems likely that, in the absence of physical cash, citizens will resort to cryptocurrency in order to escape constant surveillance. Cryptocurrencies lack regulation in most jurisdictions. Although Liechtenstein's blockchain act has entered into force on January 1, 2020, and EU countries have been obligated to follow the 5th Anti-Money Laundering Directive (AMLD5) since January 10, 2020, regulators of cryptocurrency face a number of obstacles. Apart from the AMLD5, there are no common rules for the regulation of virtual currencies. Only "a tiny fraction of Bitcoins or other digital coins"[47] are exchanged for euros. Therefore, most decision makers have not paid cryptocurrencies much attention, thus far. Now that Libra has been announced, the EU in particular seems to be increasingly concerned with cryptocurrencies. However, EU regulators have not agreed on how to treat virtual currencies, yet. In particular, cryptocurrencies could be defined as either payment services, securities, or currencies. However, the option to treat them as currencies is ruled out by most[48]. Furthermore, it has not been agreed upon whether existing rules of governing financial instruments could apply to virtual currencies. Therefore, users of virtual currencies largely operate in a legal gray area in the EU. Other jurisdictions frequently (such as Saudi Arabia, Vietnam, and Bolivia) either ban cryptocurrency entirely, or restrict them (such as China, Morocco, and Ecuador)[49]. However, data collected by the crypto trading platform LocalBitcoins show that in China, India, and Saudi Arabia, cryptocurrencies such as Bitcoin continue to be traded despite bans and restrictions[50].

# V. LIBRA

As previously mentioned, the introduction of Facebook's stablecoin Libra has motivated multiple governments and central banks to research options for their own digital currency. At the beginning of 2019, experts were still skeptical about state-backed digital currencies. The general manager of the Bank of International Settlements, Augustín Carstens, showed little enthusiasm: "Research and experimentation have so far failed to put

46 Id.

47 Guarascio, *UPDATE 1-EU Finance Commissioner Pledges to Regulate Digital Currencies* (Oct. 8. 2019), https://www.cnbc.com/2019/10/08/reuters-america-update-1-eu-finance-commissioner-pledges-to-regulate-digital-currencies.html.

48 Id.

49 Cryptonews, *Countries Where Bitcoin is Banned or Legal in 2020* (n.d.), https://cryptonews.com/guides/countries-in-which-bitcoin-is-banned-or-legal.htm.

50 Coin.Dance, *LocalBitcoins Volume Charts*, COIN DANCE (Updated Weekly), https://coin.dance/volume/localbitcoins.

forward a convincing case [...] Central banks are not seeing today the value of venturing into uncharted territory"[51]. In July, Carstens corrected his March statement and said that central bank digital currencies may be closer to being implemented than initially expected. This change of heart occurred after Facebook revealed its plans for Libra in June[52].

The Libra association is located in Geneva, Switzerland, and consists of renowned firms such as Spotify, Lyft, Vodafone, and Coinbase. Unlike other cryptocurrencies, Libra is a stablecoin, which means that its value is backed by a reserve of assets. In addition, Libra is centralized, which means that, unlike Bitcoin and other cryptocurrencies, Libra nodes (computers that verify transactions and validate the network) are controlled exclusively by the Libra Association. The fact that Libra is controlled by private companies is being criticized harshly by international experts, especially in Europe, for instance by Yves Mersch, head of the European Central Bank[53]. In line with Germany, France and the United States have also uttered their concerns. Further, Facebook's multiple data protection breaches and scandals have elicited skepticism regarding Libra, from not only a large proportion of Facebook users but also central bank officials. As a result from the extensive international criticism, some members of the Libra Association, including PayPal, Visa, and Mastercard, have withdrawn their support for the stablecoin.[54]

Apart from data protection concerns, regulators are worried that Libra will interfere with monetary policy, which is a core government function[55]. German Finance Minister Olaf Scholz argued that the issuance of a currency is a core element of state sovereignty that must not fall into the hands of private companies[56]. Facebook is not the only company attempting to venture into finance; corporations such as Google and Apple are also entering the field: Apple has created a credit card, and Google provides an electronic wallet and has announced plans for checking accounts for users of their wallet. The wallet in one's phone can be used to make, for instance, payments in stores[57]. Thus, tech firms are offering services that have traditionally been associated with banks. However, when

---

51 A. Carstens, *The Future of Money and Payments*, BANK FOR INTERNATIONAL SETTLEMENTS (MAR. 22, 2019), https://www.bis.org/speeches/sp190322.pdf.

52 M. Orcutt, *Facebook's Digital Currency May Force Central Banks to Create Their Own*, MIT TECHNOLOGY REVIEW (July 1, 2019), https://www.technologyreview.com/f/613909/facebooks-digital-currency-may-force-central-banks-to-create-their-own/.

53 Y. Mersch, *Money and Private Currencies: Reflections on Libra, European Central Bank* (Sept. 2, 2019), https://www.ecb.europa.eu/press/key/date/2019/html/ecb.sp190902~aedded9219.en.html.

54 R. Brandom, *Facebook's Libra Association crumbling as Visa, Mastercard, Stripe, and others exit.* THE VERGE (Oct. 11, 2019), https://www.theverge.com/2019/10/11/20910330/mastercard-stripe-ebay-facebook-libra-association-withdrawal-cryptocurrency.

55 Colitt & Marsh, *Facebook's Obstacles in Europe Mount as Germany Opposes Libra* (Sep. 18,2019), https://www.bloomberg.com/news/articles/2019-09-18/germany-broadens-european-front-opposing-facebook-s-libra-plan.

56 Id.

57 Wall Street Journal, *Why big tech is getting into finance*, YOUTUBE (Jan. 14, 2020), https://www.youtube.com/watch?v=0KFpUZT7g04.

Google or Apple process payments for their clients, they gather vast amounts of data, including the date and time of the payment, the vendor, and the amount transferred. This information is valuable for advertisers. The associated companies all began by offering one service or product, and then gradually widened their range and experienced rapid growth at the same time. In response, several United States' regulatory bodies have initiated antitrust investigations into Google, Facebook, Apple, and other companies. Further, the public seems to be distrustful, especially of Facebook[58].

The main question regarding Libra is whether private companies should be trusted with one's money. Private stablecoin providers have the potential to unseat banks. Banks, however, are subject to strict compliance requirements and consumer protection rules. Tech giants, on the other hand, could use their networks to monetize information, according to economists Adrian and Mancini-Griffoli of the IMF[59]. They also argue that stablecoin users risk losing their assets, and that stablecoins could undermine financial stability. Central banks, such as the ones in Singapore and China have, in response to Libra, begun to work on their own equivalents, which will be discussed in the following sections.

## VI. CENTRAL BANK-ISSUED DIGITAL CURRENCY

### A. China

The initiative for a Chinese digital currency was commenced in 2014. However, the announcement of the planned launch of Libra seems to have accelerated the process. According to Mu Chanchun, the head of the PBOC digital currency research institute, Libra could be accepted by everyone and therefore widely used as a payment tool. His fear is that it will "develop into a global, super-sovereign currency"[60]. In response, he argued in an online lecture, China would need to protect its monetary sovereignty[61]. According to Chinese officials, their aim is for the Chinese currency, the renminbi, to be used more in international finance and trade. During a speech he gave in July 2019, former central bank governor Zhou claimed that "the dominance of the dollar had eroded the economies of nations with 'weak' currencies", and warned that Libra could lead to similar outcomes[62].

Under the initiative for a Chinese digital currency, the plan is to distribute the digital money first to commercial banks. Thereafter, users and businesses will be able to register

58 Id.

59 T. Adrian & T. Mancini-Griffoli, *Digital Currencies: The Rise of Stablecoins*, INTERNATIONAL MONETARY FUND (Sept. 19, 2019), https://blogs.imf.org/2019/09/19/digital-currencies-the-rise-of-stablecoins/.

60 Chanchun quoted in Zhong, *supra* note 3.

61 Zhong, *supra* note 3.

62 Zhong, *supra* note 3.

wallets with these commercial banks, according to the PBOC[63]. The pilot digital currency will reportedly be tested in the cities Shenzen and Suzhou. For this purpose, the PBOC has partnered with several state-owned commercial banks and telecoms[64]. In the Chinese province Anhui, the government has also announced that it will "adopt blockchain technology across governmental service centers"[65]. This includes all levels of government in Anhui, which will be using blockchain, artificial intelligence, and other new technologies to offer governmental services at all times. The stated intention is to "digitize Anhui's governance infrastructure and streamline the collection and sharing of government data and resources". In December 2019, the Chinese central government had published a guideline for the Yangtze River Delta Economy Region, which Anhui is part of, to prioritize the development of artificial intelligence, blockchain, cloud computing, and other emerging technologies[66].

## Concerns

According to economist Gary Liu, the Chinese digital currency will be "highly controlled, manageable, and decided by the central government"[67], and thus diverge from the original concept of cybersecurity. According to a senior bank official, the Chinese digital currency will not seek to "gain full control of information belonging to the general public"; instead, the PBOC claims the goal is to balance the authorities' need for information and privacy concerns[68]. China has suggested that it will not provide marketers with spending information; authorities, however, will have access[69].

Users are already required to authenticate their names and identities with the banks and electronic payment companies that will distribute the digital currency. Further, the central bank will be able to view transaction data[70]. Experts claim that in contrast to Bitcoin

63 C. Wan, Report: China's Central Bank to Test Digital Currency in Two Cities, Partnering with State-Backed Commercial Banks and Telecom Giants, THE BLOCK (Dec. 9, 2019, 12:35 AM EST), https://www.theblockcrypto.com/post/49659/report-chinas-central-bank-to-test-digital-currency-in-two-cities-partnering-with-state-backed-commercial-banks-and-telecom-giants.

64 Y. Katri, *China's Digital Currency "Progressing Smoothly," Says Central Bank*, THE BLOCK (Jan. 6, 2020), https://www.theblockcrypto.com/linked/52092/chinas-digital-currency-progressing-smoothly-says-central-bank?utm_source=newsletter&utm_medium=email&utm_campaign=2020-01-12.

65 Y. Cheng, *Chinese Local Government Eyes Adoption of Blockchain for Service Centers*, THE BLOCK (Jan. 8, 2020), https://www.theblockcrypto.com/linked/52200/chinese-local-government-eyes-adoption-of-blockchain-for-service-centers?utm_source=newsletter&utm_medium=email&utm_campaign=2020-01-08.

66 Id.

67 Liu quoted in Zhong, *supra* note 3.

68 A. John & K. Coghill, *China's Digital Currency Not Seeking "Full Control" of Individuals' Details: Central Bank Official*, REUTERS (Nov. 12, 2019), https://www.reuters.com/article/us-china-markets-digital-currency/chinas-digital-currency-not-seeking-full-control-of-individuals-details-central-bank-official-idUSKBN1XM0H2.

69 Zhong, *supra* note 3.

70 Zhong, *supra* note 3.

and Libra, the currency seems to have been designed to provide Beijing "with unprecedented oversight over money flows, giving Chinese authorities a degree of control over their economy that most central banks do not have"[71]. During a conference in Singapore, Mu Changchun assured the public that users of the digital currency will continue to have privacy in their transactions. At the same time, he claimed that the PBOC will find a balance between "controllable anonymity" and anti-money laundering (AML), counter terrorist financing (CFT), tax issues, online gambling, and any other electronic criminal activities[72].

Changchun's statements are questionable: "controlled anonymity" seems a paradox in itself. After all, the government or law enforcement agencies will need to sort through all user information in order to be able to identify AML or CFT breaches. Flex Yang, the founder of a Hong Kong-based financial provider of cryptocurrencies, Babel Finance, argues that "currencies should be neutral"; without anonymity, he argues, the money cannot be considered a currency, "it can only be a payment vehicle"[73]. However, China could agree not to save user data, as long as the person in question has not broken the law. Critics of the new digital currency also argue that China's persecuted minorities will "face even harsher conditions under a fully integrated financial system controlled by the government"[74]. In an interview with *Coindesk*, an anonymous Chinese bitcoiner stated that a totalitarian state could use blockchain to track every person and their actions, and to enforce strict currency controls. They go on to talk about how their parents (Christian missionaries) have been subject to constant surveillance by the Chinese government. They claim that, once, their WePay and AliPay accounts were frozen. If they had not had cash, they would have been left with no money[75]. These statements raise concerns that the complete digitalization of money would leave political opponents and minorities vulnerable to the repercussions of censorship.

## B. United States

In the United States, lawmakers have asked the Federal Reserve to consider the creation of a digital dollar. On September 30, 2019, Rep. French Hill and Rep. Bill Foster sent a letter to Federal Reserve Chairman Jerome Powell in which they expressed their concerns regarding risks to the US dollar if another nation or private company were to create a widely employed cryptocurrency. In particular, they emphasized their concern that the primacy of the US dollar could be in jeopardy in case of a wide adoption of digital fiat

71 John & Coghill, *supra* note 68.

72 John & Coghill, *supra* note 68.

73 Yang quoted in Zhong, *supra* note 3.

74 L. Cuen, *Bitcoin Dissident Sees Dark Warnings in China's Blockchain Push*, COINDESK (Oct. 31, 2019, 10:20 AM UTC), https://www.coindesk.com/bitcoin-dissident-sees-dark-warnings-in-chinas-blockchain-push.

75 Id.

currencies[76]. Their letter also specifically mentioned Libra. On October 24, 2019, the Federal Reserve stated that it is planning to respond to the letter. Former Federal Deposit Insurance Corporation Chair Sheila Bair also suggested that the Federal Reserve should explore the option of creating a digital currency in order to avoid being disrupted by the private sector or other nations[77].

## C. European Union

In September 2019, Germany and France responded to the announced launch of Libra by claiming that the stablecoin "posed risks to the financial sector that could block its authorization in Europe"[78]. Both countries support the development of an alternative public cryptocurrency. French finance minister Bruno Le Maire and German finance minister Olaf Scholz released a joint statement at a meeting of euro zone finance ministers in Helsinki, in which they argued that virtual currencies pose risks to financial stability, consumers, and monetary sovereignty[79]. According to European Central Bank (ECB) board member Benoît Cœure, Libra constituted a "wake-up call"[80]. Accordingly, Libra has motivated new efforts to launch an ECB-backed project, TIPS, in the euro zone. Banks, however, have responded to this project with apprehension. The ECB seems to also be planning a central bank-issued digital currency. According to Cœure, consumers would be able to use electronic cash, which would be directly deposited at the ECB. Thus, there would be no need for bank accounts, clearing counterparties, or financial intermediaries. As a consequence, transaction costs would decrease. In light of these ambitions, opposition from banks is likely. At the same time, the technical feasibility "remains to be seen"[81]. In November 2019, Cœure told a conference in Brussels that "a central bank digital currency could ensure that citizens remain able to use central bank money, even if cash is eventually no longer used"[82].

## D. Venezuela

In 2018, Venezuela, which is plagued by hyperinflation, launched its cryptocurrency called petro. Critics claim that it represents an attempt to collect dollars and open up foreign business channels. The price of petro is based on the oil price; one petro is supposed to

---

76 F. Hill & B. Foster, *Letter to Jerome H. Powell*, COINDESK (Sept. 30, 2019), https://www.coindesk.com/wp-content/uploads/2019/10/Foster-Hill-US-Crypto.pdf.

77 N. De, *US Lawmakers Ask Fed to Consider Developing a "National Digital Currency"*, COINDESK (Oct. 2, 2019, 23:08 UCT), https://www.coindesk.com/us-congressmen-ask-fed-to-consider-developing-national-digital-currency.

78 Guarascio, *supra* note 47.

79 Guarascio, *supra* note 47.

80 Cœure quoted in Guarascio, *supra* note 47.

81 Guarascio, *supra* note 47.

82 B. Cœure, *Towards the Retail Payments of Tomorrow: A European Strategy*, EUROPEAN CENTRAL BANK (Nov. 26, 2019), https://www.ecb.europa.eu/press/key/date/2019/html/ecb.sp191126~5230672c11.en.html.

cost as much as one oil barrel, which is about $US60[83]. Petro is also backed by Venezuela's oil reserves[84]. Although petro is claimed to be a cryptocurrency, it is supervised and controlled by the federal authority for the supervision and control of cryptocurrencies, which conflicts with the fact that cryptocurrencies are generally decentralized and transparent[85]. It had been expected that Venezuelans would not have much interest in buying petro, because of the high rates of poverty or lack of access to US dollars. Therefore, it has been argued that petro is mainly a vehicle that allows corrupt officials, politicians, and companies to transfer their assets out of the country. It is also argued that there is no real incentive for investors to buy petro, as three dozen regime members have been sanctioned by the US[86]. Other sources state that petro was launched to circumvent these sanctions and overcome liquidity shortages[87].

Thus far, petro has been unsuccessful in winning over investors: the currency has, in fact, been banned by the United States. Risk-ranking bodies have also labeled it a "scam"[88]. Although petro has failed, other cryptocurrencies such as Bitcoin see an increase in their trade[89] (See e.g., Coin.Dance, 2020). Many Venezuelans keep physical dollar bills to retain their assets, which makes them vulnerable to burglary[90]. Therefore, Venezuelans have resorted to cryptocurrency. There is even a popular local trade, LocalBitcoins, that facilitates exchanges between Bitcoin and bolivars, the national currency[91]. In an effort to revive petro, the Venezuelan president, Nicolas Maduro, has decreed that all airlines flying from Caracas must purchase their fuel using petro and that the currency is to be used to pay for state document services such as passports[92]. When Maduro approved bonuses for public employees and pensioners in December 2019, these were also paid out in petros. However, the petros were quickly exchanged for bolivars, and then for other currencies. At the beginning of 2020, the government blocked the exchange of bolivars for petros[93].

## VII. TOWARD A CASHLESS SOCIETY?

---

83 A. Busch, *Venezuelas Kryptowährung Petro ist ein Verzweifelter Versuch an Ausländische Gelder zu Kommen* [in German], NEUE ZÜRCHER ZEITUNG AG (Feb. 21, 2018), https://www.nzz.ch/wirtschaft/potemkinscher-petro-ld.1359430.

84 France24, *Maduro Bids to Revive Venezuela's 'Petro' Cryptocurrency*, FRANCE24 (Jan. 15, 2020), https://www.france24.com/en/20200114-maduro-bids-to-revive-venezuela-s-petro-cryptocurrency.

85 Busch, *supra* note 83.

86 Busch, *supra* note 83.

87 France24, *supra* note 84.

88 France24, *supra* note 84.

89 For example, see Coin.Dance, *supra* note 50.

90 Orcutt, *supra* note 2.

91 Orcutt, *supra* note 2.

92 France24, *supra* note 84.

93 France24, *supra* note 84.

According to experts, digital money has the potential to replace cash altogether. Sweden is one example of an almost cashless society. According to the Swedish central bank, the number of payments made using cash is expected to drop to 0.5% by 2020[94]. Further, South Korea intends to phase out cash in 2020[95]. Even in the UK, where cash continues to be rather popular, bus fares can no longer be paid in cash[96]. Many citizens in comparatively cashless societies utilize mobile payment systems provided by banks and fintechs (e.g., Apple Pay or Chinese providers AliPay and WeChat Pay) or credit cards. Naturally, these companies have an interest in promoting a cashless society because they collect transaction fees from their customers[97]. Some financial service providers, including Visa, have launched advertisements and media campaigns to convince customers to give up cash for card payments[98]. Central banks have an interest in a cashless society, as well, as they would be able to "grow the monetary policy tools at their disposal" and "impose negative interest rates across the whole economy"[99]. Further, economist Joseph Stiglitz argued that cash should be abolished in order to hinder financial corruption and tax evasion[100].

Online, the use of cash has never been possible. Because of the fact that commerce is increasingly relocating to the internet, "the proportion of intermediated payments grows concomitantly"[101]. As online retail is becoming more popular, intermediaries will inevitably have better access to information about buying habits[102]. However, as shown by Bech et al.,[103] on a global scale, the demand for cash has not decreased. A report by the Bank for International Settlements (BIS) found that cash demand, which is measured by proxy through cash in circulation, has increased among the majority of the 46 national economies in its sample. In addition, out of 24 nations investigated, only Sweden and Russia were shown to exhibit signs of substituting cash payments with card payments. The remaining 22 countries showed an increase in both cash demand and online payments with

94 J. Henley, *Sweden Leads the Race to Become Cashless Society*, THE GUARDIAN (June 4, 2016, 16:00 BST), https://www.theguardian.com/business/2016/jun/04/sweden-cashless-society-cards-phone-apps-leading-europe.

95 P. Jenkins, *"We Don't Take Cash": Is This the Future of Money?*, FINANCIAL TIMES (May 9, 2018), https://www.ft.com/content/9fc55dda-5316-11e8-b24e-cad6aa67e23e.

96 Transport for London, *Cash Free Buses*, TRANSPORT FOR LONDON (no date), https://tfl.gov.uk/modes/buses/cash-free-buses.

97 B. Scott, *The War on Cash*, NESTA (Aug. 19, 2016), https://thelongandshort.org/society/war-on-cash.

98 P. Jenkins, *supra* note 95.

99 Brito, *supra* note 6.

100 R. Chainey, *The US Should Get Rid of Cash and Move to a Digital Currency, Says Nobel Laureate Economist*, WORLD ECONOMIC FORUM (Jan. 17, 2017), https://www.weforum.org/agenda/2017/01/the-us-should-get-rid-of-cash-and-become-a-digital-economy-says-this-nobel-laureate-economist/.

101 Brito, *supra* note 6.

102 Brito, *supra* note 6.

103 M.L. Bech et al., *Payments are A-changin' but Cash Still Rules*, BANK FOR INTERNATIONAL SETTLEMENTS (Mar. 11, 2018), https://www.bis.org/publ/qtrpdf/r_qt1803g.htm.

the use of cards, which suggests that the unique features of cash are valued[104].

## A. Benefits of a Cashless Society

In *The Curse of Cash*, economist Kenneth Rogoff argues that cash is "making us poorer and less safe". In line with Bech et al., Rogoff shows that even though cash is being used less frequently, the amount of cash in circulation is actually growing. According to him, this cash is being used for tax evasion, terrorism, corruption, human trafficking, the drug trade, and a "massive global underground economy". This could also affect monetary policy, according to Rogoff. After the 2008 global financial crisis, central banks were not able "to stimulate growth and inflation by cutting interest rates significantly below zero for fear that it would drive investors to abandon treasury bills and stockpile cash"[105].

Compliance officers around the world will likely agree with Rogoff in that cash represents an immense risk factor for all sorts of crime. From a compliance perspective, cash poses tremendous threats to public safety as it is highly anonymous and non-transparent, which makes it well suited to crime and money laundering or terrorism financing. Corruption, particularly bribery, is another concern relating to cash. With money laundering, cash would be generated during a predicate offense. A drug dealer in Zurich, for instance, will accept cash from their clients, with no paper trail or digital record of the transaction. The same is true for bribery and terrorism financing.

Although financial institutions and banks are subject to strict compliance measures, cash-intensive businesses are frequently excluded from these measures. Therefore, money launderers and terrorism financiers are increasingly relocating to less-regulated sectors. Our 2016 quantitative study showed that, out of the 153 responding compliance experts, 74.5% agreed that money launderers are relocating to less-regulated sectors[106]. Therefore, it can be assumed that, in a cashless society, it would be much more difficult for criminals to continue their illicit activities without being detected. After all, every digital transaction would be traceable, which in itself could serve as a deterrent for criminals. In addition, they would need to find new methods to be able conduct untraceable transactions.

## B. Risks of a Cashless Society

According to Scott A. Shay[107], chairman of Signature Bank, the US government frequently seizes money from its citizens before conducting an investigation, even if government staff members have no proof of wrongdoing. When a person's or company's assets are seized, the defendant frequently has no other option than to settle. In one instance,

---

104 Id.

105 K. ROGOFF, THE CURSE OF CASH 1 (Princeton University Press) (2016).

106 Teichmann, *supra* note 12, at 85.

107 S.A. Shay, *Cashless Society: A Huge Threat To Our Freedom*, CNBC LLC (Dec. 12, 2013), https://www.cnbc.com/2013/12/12/cashless-society-a-huge-threat-to-our-freedomcommentary.html.

which was argued before the Supreme Court, the government had seized all the money of a small family-owned grocery store because its cash deposits were below the $US10,000 threshold, which triggered a report to the government. As a result, the defendants were deprived of money they needed to defend themselves. In such cases, defendants often are under pressure to settle or plead guilty[108] owing to the fact that they have no access to their financial assets. However, they can use cash to finance their daily life, so that they do not go hungry. In a cashless society, the freezing of a family's financial assets could accordingly have fatal consequences.

Algorithms that instantaneously review and evaluate financial transactions are available, and in use by credit and debit card firms. The technology is typically used to issue fraud alerts following unusual consumer purchases. In 2010, Mastercard and Visa banned online-betting payments in response to pressure from the US government. Thus, gambling sites struggled to continue operating, regardless of their location or legality. At present, these restrictive mechanisms can be circumvented through the use of cash. In a cashless society, however, the government would have "unprecedented access to information and power over citizens", according to Shay[109].

In addition, it has become easier for governments to gather information. JP Morgan is one of the largest US banks; its size is that of 3,000 smaller banks combined, and the top four US banks have control over circa 60% of US banking deposits. Thus, there are fewer access points for the government. There are compliance hurdles in place for banks that wish to deal with certain customers, which make business relations with them expensive. In response, some banks, including JP Morgan, refrain from dealing with these clients altogether. In this manner, the government can prevent certain individuals or companies from accessing the financial system[110]. Therefore, it could be argued that a cashless society could lead to extensive governmental control over human behavior.

Shay calls this phenomenon, which he describes as economic singularity, "econgularity". He defines econgularity as the moment in time when technological surveillance, big data manipulation, and a cashless economy converge[111]. In light of the data presented in section 4.0, this scenario could potentially be approaching faster than expected. With econgularity, Shay argues that it would be possible for government staff members to order the freezing of funds or decline withdrawals or payments for individuals who are suspected of misconduct or those are political opposers. Before the person is able to access their funds again, their case might need to be reviewed, which would take time. In the meantime, the individual "might starve to death". In addition, anyone suspected of helping the person could be cut off from accessing their assets, as well[112]. Naturally, a cashless society will not

108 Id.

109 Id.

110 Id.

111 Id.

112 Id.

take this form in all jurisdictions; however, some governments could take the opportunity to exert greater control over their citizens. According to crypto expert Jerry Brito, the death of cash will inevitably cause "the birth of perfect financial control"[113].

### C. Responses

In the United States, citizens have begun to argue that cashless businesses violate their civil rights. Cities such as San Francisco, Washington D.C., and Philadelphia have therefore ruled these businesses out. In New York City, legislation that prevents retail establishments from refusing to accept cash payments was introduced in February 2019[114]. In August, the law was rescinded, but reintroduced in December 2019 (The New York City Council, n.d.). As of January 2020, the New York Council has voted to ban cashless stores and restaurants[115], which means cashless businesses could face fines of up to $US500 per violation. In addition to the fear of governmental surveillance and censoring of payments, some opponents have also argued that cashless businesses discriminate against low-income people, who are often undocumented immigrants or people of color[116]. In New York City, 25% of underbanked citizens and 12% of unbanked citizens are people of color, whereas only 3% of white New Yorkers are unbanked[117]. This raised the question of whether cashless businesses are a manifestation of racial discrimination. This could also be problematic for every other demographic that does not have access to a bank account (e.g., homeless or unemployed persons). Businesses that operate cash-free argue that a ban of cash payments increases efficiency, saves money and time by cutting out the need for armored vehicles for transportation, and protects their employees against robbery[118].

## VIII. DISCUSSION

Ultimately, an abandonment of cash could facilitate more effective crime prevention and prosecution. However, we suggest that replacing cash with a digital form is rather unnecessary: the development of digital cash requires an abundance of resources, including time, money, human resources, and materials. In addition, once established, the technology will need to be maintained, which will require further resources. If the intention is to create digital currency with the same characteristics and anonymity as physical cash, there

---

113 Brito, *supra* note 5.

114 R. Bellan, *As More Cities Ban Cashless Businesses, New York Wants to Follow* (Mar 6, 2019), https://www.citylab.com/equity/2019/03/cashless-cash-free-ban-bill-new-york-retail-discrimination/584203/.

115 C. Jones, *New York Says Don't Ditch Your Cash: City is Latest to Ban Cashless Restaurants, Stores* (Jan. 24, 2020), https://eu.usatoday.com/story/money/2020/01/23/new-york-city-bans-cashless-businesses/4551974002/.

116 Bellan, *supra* note 114.

117 Federal Deposit Insurance Corporation, *FIC National Survey of Unbanked and Underbanked Households – Executive Summary*, FEDERAL DEPOSIT INSURANCE CORPORATION (Oct., 2018), https://www.fdic.gov/householdsurvey/2017/2017execsumm.pdf.

118 Bellan, *supra* note 114.

is no use in replacing physical cash in the first place. Cryptocurrencies, on the other hand, are useful primarily for criminals, as they do not require the transacting parties to meet at one location. Thus, they facilitate discreet payments without personal contact. When it comes to blockchain, the technology shows great potential in the area of smart contracts. These could enable legal transactions; in particular, trading with rights and securities could be simplified.

Although at present a cashless society is not yet in sight, an increasing number of payments are conducted via credit or debit card. Statistics relating to credit card and cash spending are indicators of consumer spending habits, which could also be used to analyze the broader economy as a whole[119]. A 2017 study conducted by global payments company TSYS, which investigated consumer payment, has shown that, currently, debit cards are the most popular payment method. In particular, out of 1,222 consumers, 54% chose debit cards as their preferred form of payment, while 26% selected credit cards, and 14% stated that they preferred cash. It was also shown that consumers are becoming increasingly interested in mobile wallets[120]. In 2016, global analytics and advice firm Gallup found that Americans are using increasingly less cash – in 2011, 36% of analyzed Americans reported that they made almost all purchases using cash; in comparison, this number had shrunk to 24% in 2016[121]. These findings are consistent with a multitude of other surveys. There are, however, nations that diverge from this trend: Germany is the most prominent example of a country where residents continue to prefer cash over credit or debit card payments, mainly for privacy reasons[122].

In light of these findings, financial service providers will see themselves presented with increasingly high compliance requirements. With regard to data protection compliance, it is of immense importance that customer data is handled responsibly. This includes accurate encryption and theft-prevention measures. At the same time, customers must be made aware of how their data is used and who has access to it. Herein, it should be ensured that customers have the option to opt out of providing their data for certain purposes such as advertisement. A study by researchers from MIT, UCL, and Aarhus University has recently shown that out of 10,000 websites, only 11.8% meet minimal requirements of the GDPR. In particular, many websites make it difficult for users to opt out of tracking. Pop-up windows for cookie consent are often designed so that rejecting tracking is much more difficult than consenting to it – in most cases, there is an option to "accept all" but none to "reject all". In addition, 32.5% of the surveyed websites bypass EU law via implicit consent, which assumes that failure to respond to a pop-up window or the visiting of the

---

119 M. Shepherd, *19 Cash vs Credit Card Spending Statistics*, FUNDERA INC (Dec. 31, 2019), https://www.fundera.com/resources/cash-vs-credit-card-spending-statistics.

120 TSYS, *Consumer Payment Study*, 7, 38, TOTAL SYSTEM SERVICES INC (Mar., 2018), https://www.tsys.com/Assets/TSYS/downloads/rs_2017-us-consumer-payment-study.pdf.

121 A. Swift & S. Ander, *Americans Using Cash Less Compared With Five Years Ago*, GALLUP (July 12, 2016), https://news.gallup.com/poll/193649/americans-using-cash-less-compared-five-years-ago.aspx.

122 M. Campbell, *Germany is Still Obsessed with Cash*, BLOOMBERG (Feb. 6, 2018), https://www.bloomberg.com/news/features/2018-02-06/germany-is-still-obsessed-with-cash.

site alone implies consent[123]. When handling sensitive customer data, practices such as the assumption of implicit consent or potential data breaches could lead to significant reputational damages for the institution if thematized by the media.

In the absence of predefined standards, however, financial institutions will also face a number of unresolved questions. In order to ensure legal security and prevent compliance scandals, these questions must be addressed urgently, so that institutions do not operate in dangerous legal gray areas. On January 1, 2020, Liechtenstein's new blockchain act (German: Token- und VT-Dienstleister Gesetz, TVTG) entered into force. Liechtenstein is one of the first jurisdictions to regulate blockchain and its potential uses, which includes financial services. With the introduction of the TVTG, the Due Diligence Act (German: Sorgfaltspflichtgesetz, SPG) has been amended so that due diligence requirements include service providers for virtual currencies[124]. Due diligence measures aim to prevent money laundering, terrorism financing, and organized crime.

## IX. CONCLUSION

Although cryptocurrencies, led by Bitcoin, have been around for over ten years now, up until recently most central banks and governments seemed to perceive no significant threat to traditional money from digital currency. This sentiment has changed drastically since the planned launch of Libra was announced by Facebook. Overall, reactions to Libra have been overwhelmingly negative: multiple central bank officials and politicians have expressed concerns regarding implications for privacy and monetary policy. In particular, the experts have argued that money should not be issued by a private company, but by a sovereign entity, i.e., a central bank. Central banks are also concerned that Libra could become a widely used payment method that is preferred over governmental currency. In response, multiple central banks have announced that they will begin developing their own digital currency, or have accelerated their already existing research efforts. China will likely be the first nation to issue a digital currency. However, China's ambitions are viewed critically by the public: the country is known to use new technologies for the surveillance of its citizens; as a result, opponents fear that the digital currency will be used to surveil and control citizens.

In particular, the PBOC seems to intend to replace physical cash with digital cash. Digital cash, however, can never be as private as physical cash; accordingly, the public does not seem convinced that their data will not be used for purposes other than processing payments. In addition, digital cash is not censorship-resistant, which means that certain groups of people (e.g., minorities or homeless persons) could be prevented from accessing the monetary system. These concerns apply to cashless societies in general. However, a

123 M. Nouwens et al., *Dark Patterns After the GDPR: Scraping Consent Pop-ups and Demonstrating Their Influence*, CORNELL UNIVERSITY (Jan.8, 2020), https://arxiv.org/abs/2001.02479.

124 Sorgfaltspflichtgesetz (Dec. 11, 2008)[in German], Art. 3 Sec. 1 (f).

cashless society would come with the advantage that organized crime would be significantly hindered. As a consequence, money laundering would also become a less pressing issue. However, in this scenario, it must be ensured that there is an appropriate legal framework for financial service providers to operate within, so that data protection and compliance breaches can be prevented. Ultimately, only time will tell whether cash will, at some point, be replaced by digital currency. Totalitarian governments could use digital currency to surveil the public, marginalize political opponents, or even prevent citizens from accessing the financial system altogether. Therefore, the creation of an ethical, internationally valid framework is crucial. The establishment of such a framework would naturally be highly challenging. Therefore, the international community should ensure that countries that seek to violate human rights through their use of digital currency are penalized with hard sanctions, and that their citizens are protected from governmental control.

CEJ
COMPLIANCE
ELLIANCE
JOURNAL

# IS THIS OUR PLUMBUS? AN EXPLORATION OF CRYPTO AND VIRTUAL CURRENCIES THROUGH A COMPLIANCE LENS

Sharon Kits Kimathi

## AUTHOR

*Sharon Kits Kimathi is Editor of Fintech Futures and Banking Technology since May 2019, having been Deputy Editor at the International Financial Law Review (IFLR) and a capital markets Reporter at Global Capital and mtn-i. She has worked as a Paralegal for Freshfields Bruckhaus Deringer; Legal Compliance Associate for Goldman Sachs; and Paralegal at Reed Smith LLP. It was conducting legal research for fintech clients at the latter which prompted a shift in career trajectory, away from the legal profession and towards specialist research and journalism from September 2016. She has appeared on television discussing Libra and cryptocurrency on TRT and has moderated and participated as a panellist and speaker at various fintech industry events such as the Cybersec: European Cybersecurity Forum in Poland and FinovateEurope in Berlin. With special thanks to Jamie Ranger, DPhil candidate in the Department of Politics at St. Hugh's College, University of Oxford.*

## ABSTRACT

*In this comment piece, I will seek to examine the relationship between cryptocurrencies and virtual currencies from a compliance perspective. I will tie this to the underlying theme from multiple studies, that a lack of knowledge of these products means more needs to be done by policymakers and the crypto industry to form cohesive and understandable standards that unearth what these products are, how they are used and how compliance analysts can be best supported to apply best practice procedures when conducting due-diligence checks. I will seek to lay out the advantages and disadvantages of recent developments and explore the challenges they pose on a socio-economic and macro level. This piece dissects the topic through four chapters.*

*The first ties it into developments that unfolded during the global financial crisis, the use of collateralized debt obligations and other derivatives-based financial instruments, ultimately showing how a lack of knowledge was an underlying theme within the banking system during the 2008 global financial crisis. The second chapter combines the theme of knowledge and awareness of a product with the way in which people view cryptocurrency and digital coins, including regulators, courts and policymakers.*

*The third explores recent developments from international central banks and governments, from sanctioned countries using of the product to help their citizens to international alliances forming across the globe in support of central-bank digital currencies.*

*The final chapter unpacks the advantages and disadvantages of using these financial instruments, from countries in the global south suffering from scams to the pressure it takes on energy efficiency, concluding that more needs to be done to educate users, regulators and everyone in between for the success of the digital currency to be fully realized.*

## TABLE OF CONTENTS

## I. A HISTORY LESSON FROM THE DERIVATIVES MARKET

Cryptocurrencies. Virtual currencies. Digital coins. Studies from ING[1] and St Andrews University[2] reveal that, "while most of us now know something about these terms, many of the details are still a little sketchy." For me, the term cryptocurrency or virtual currency is ingrained somewhere in my brain that leads me to conjure up images from the popular animated TV show, *Rick & Morty*. I believe it will provide some insight on how people view 'crypto' in general. In the show, our titular characters sit down to watch alien television through the use of their 'interdimensional cable' device and witness the following:

> *"Plumbuses – Everyone has a Plumbus in their home. First, they take the dinglebop, and they smooth it out, with a bunch of Schleem. The Schleem is then repurposed for later batches. They take the dinglebop and push it through the Grumbo, where the Fleeb is rubbed against it. It is important that the Fleeb is rubbed, because the fleeb has all of the fleeb juice. Then a Schlommy shows up and he rubs it and spits on it. They cut the fleeb. They are several hizzards in the way. The blamphs rub against the chumbles. And the plubus and grumbo are shaved away. That leaves you with a regular old Plumbus."*[3]

Rick, the genius scientist and multidimensional traveler, nods sagely, whilst his oblivious grandson Morty, is as perplexed as the audience. Whilst this mock documentary is revealing the inner machinations of a nonsense object being produced through unintelligible steps using unknown ingredients, it leaves us completely in the dark without a frame of reference. "Huh," Rick says, "always wondered how Plumbuses got made."

In my experience as a journalist and former legal and compliance analyst, people are often enticed by financial products that sound ground-breaking. Who doesn't wish to be the first to uncover something special? Being part of a cultural sea-change, being the right side of a technological paradigm shift, and generally appearing to have some insider knowledge on future trends, are all (understandably) valued in the industry. However, this focus on the symbolic value of products rather than their immediate value calls to mind the 'father of postmodernism', French sociologist and cultural theorist Jean Baudrillard, who once wrote:

> *"Far from the primary status of the object being a pragmatic one which would subsequently come to overdetermine a social value of the sign, it is the sign exchange value*

---

1 Jessica Exton, *Cryptocurrencies: Curiosity and confusion among consumers*, ING (Sep. 18, 2019). https://think.ing.com/articles/sizing-up-the-money-revolution-crypto-bitcoin-currencies-digital/

2 Georgios A. Panos & Tatja Karkkainen, *Financial Literacy and Attitudes to Cryptocurrencies*, WORKING PAPERS IN RESPONSIBLE BANKING & FINANCE, WP № 20-002, pg 6 (2020).

3 Rick & Morty, season 2, episode 8, "Interdimensional Cable 2: Tempting Fate". Directed by Juan Meza-León. Written by Dan Guterman, Ryan Ridley and Justin Roiland, aired September 20 2015, on [adult swim].

*(valeur d'echange signe) which is fundamental – use value is often no more than a practical guarantee (or even a rationalisation, pure and simple) [...] An accurate theory of objects will not be established upon a theory of needs and their satisfaction, but upon a theory of social prestation and signification."* [4]

Baudrillard's intervention into the political economy debate between Marxists and classical liberal interpretations of value added a sociological dimension. Objects are bought and displayed as much for their sign-value, i.e. prestige or status, as their use-value, and that the phenomenon of sign-value has become an essential constituent of the commodity and consumption in contemporary consumer society.[5] This can be witnessed from early collectors of Fabergé eggs in 19th century Imperial Russia through to Gen-Z's obsession with the (intentionally falsely scarce and commercially hyped) Supreme brand – everyone wants to get in on "the next big thing", and sometimes that next big thing has value based on hype rather than utility.

But how would this translate when working behind a compliance desk at a bank? During my time working at the bank, a client had signed up for the first set of weather derivatives that I had encountered. For me, it was puzzling. Why would you put an 'option' or a 'forward' on the weather? This seemed perplexing and excessive. I thought that this must be the first ever occasion that someone convinced someone else to purchase such a product. I was sorely mistaken. In fact, weather derivatives had been around since the 1990s as a tool that farmers could opt for as opposed to insurance in order to 'price-in' certain weather affecting their crops – from an unexpected dry season to flooding.[6] However, the client in this instance was a high-risk hedge fund based in the Cayman Islands that was making various bets on what they deemed as high-risk products to receive the highest yields for their clients.

At the time, people in the team were only required to make the appropriate anti-money laundering (AML), know your client (KYC), market research, due-diligence, contractual and legal capacity assessments for us to be comfortable that there were no underlying risks we had not considered for the trade to go through. But nowhere within the process was it a legal requirement for any team member to demonstrate the requisite knowledge or understanding of the product. I simply went out of my way to undertake a form of 'extra-curricular' reading to fully get up to speed with what was being asked of me. This in itself is a risk.

---

4 JEAN BAUDRILLARD, FOR A CRITIQUE OF THE POLITICAL ECONOMY OF THE SIGN, pg 2, (St. Louis, Mo: Telos press Ltd., 1981).

5 Douglas Kellner, *Jean Baudrillard*, THE STANFORD ENCYCLOPEDIA OF PHILOSOPHY (Apr. 7, 2020) https://plato.stanford.edu/archives/win2019/entries/baudrillard/.

6 Sarfraz Thind, *As Temperatures Tumble in North America, Weather Derivatives Warm Up*, INSTITUTIONAL INVESTOR, (Apr. 7, 2020) https://www.institutionalinvestor.com/article/b14zbksjmn4504/as-temperatures-tumble-in-north-america-weather-derivatives-warm-up.

The lack of understanding of financial products – be it back or front-office – within banking has led to catastrophic consequences. During the run-up to the subprime mortgage crisis, Fabrice ("Fabulous Fab") Tourre, a former Goldman Sachs trader, sent an email to his girlfriend at the time who was also an employee at the bank in January 2007. His email stated: "Only potential survivor, the fabulous Fab ... Standing in the middle of all these complex, highly leveraged, exotic trades he created without necessarily understanding all of the implications of those monstrosities!!!" But that wasn't all. Tourre admitted to his lack of understanding of these financial products in yet another email sent in March 2007, referring to the financial products he worked on as "pure intellectual masturbation, the type of thing which you invent telling yourself: 'Well, what if we created a "thing", which has no purpose, which is absolutely conceptual and highly theoretical and which nobody knows how to price?'" His understanding of these financial products shows a lack of awareness of what they actually are and do.

Recall Baudrillard once again: trading something that no longer holds value in of itself, but has value depending on how it communicates the illusion of value; a copy of a copy of a copy. Similarly, cryptocurrency wishes to disavow or even transcend conventional currency, but is utterly reliant on such currencies as a reference in order to describe how they work to prospective investors. Despite their libertarian rhetoric, the jackpot for a cryptocurrency is to demonstrate its popularity amongst a core base of early investors such that it may be considered a viable option for established financial houses: selling the glamour of revolution with the security of the state. However, in the case of these derivatives, these tools were not just theoretical; they had serious real consequences that affected real people and their lives. Tourre's emails were admitted in court during a civil case brought by the Securities and Exchange Commission (SEC) after the global financial crisis, where he was found guilty for his role in a mortgage deal that cost investors $1 billion. This was because of a financial product – Abacus – that was created by the hedge fund Paulson & Co. The product is widely known as a collateralized debt obligation (CDO), and thanks to various long reads in broadsheet newspapers in the immediate aftermath of the 2008 financial crisis, and the explanation by pop-star Selina Gomez (with glamorous assistant Professor Richard H. Thaler) in the movie 'The Big Short', there has been an uptake in mainstream understanding of such complex financial instruments. Unfortunately for the financial industry, and their compliance analysts, a working knowledge of the risks of certain products prior to their becoming midwives to misery is infinitely more preferable.

This has been a trend for the derivatives product since its inception. "There is evidence of the use of derivatives in the 17th century in Holland and in Japan. Derivatives were already considered suspicious."[7] And that isn't the only example: gambling, betting or speculating on movements in securities or commodities prices without actually owning the referenced security or commodity was seen as early as 1829, known as 'stockjobbing', an early version of short-selling which was outlawed in New York. "The Stock Jobbing Act was ultimately repealed in 1858 because it was overly broad and captured legitimate forms of

7 Gunther Capelle-Blancard. *Are Derivatives Dangerous? A Literature Survey,* ÉCONOMIE INTERNATIONALE, 123(3), 67-89 (2010).

speculation. However, the question of whether to allow bets on security and commodity prices outside of organized exchanges continued to be an issue."[8]

Although derivatives might not be inherently dangerous, the suspicion of the tool emerges from a lack of complete and utter understanding of what it is and its uses. The emergence of powerful new technological breakthroughs and the enhancements of these financial products only lead to greater complexity. History has shown us that the more complicated financial instruments become, the greater the risk it can pose. A lack of understanding of what these products are from investors, traders, consumers and regulators can lead to damaging consequences. Furthermore, if a product appears unintelligible from its marketing materials, a compliance analyst should not be afraid to operate under the assumption that this unintelligibility may be deliberate.

## II. LEGAL AND REGULATORY TREATMENT OF CRYTOCURRENCIES

A cryptocurrency is defined as virtual or digital money which takes the form of tokens or coins. Financial instrument-wisdom-provider, *Investopedia*, defines the 'crypto' in cryptocurrencies as a complicated cryptography which allows for the creation and processing of digital currencies and their transactions across decentralized systems. "Alongside this important crypto feature of these currencies is a common commitment to decentralization; cryptocurrencies are typically developed as code by teams who build in mechanisms for issuance (often, although not always, through a process called "mining") and other controls."[9]

Cryptocurrencies and digital coins have a floating reliance on future prestige because the idea is that you are investing in something that *might* derive value in the future and distils an air of status once it does appreciate in value in the markets. An extract below from St Andrew's study highlights that the poorer candidates were actually more likely to invest in cryptocurrencies, viewing it as aspirational and ahead-of-the-curve. In other words, the association with complex financial manoeuvering, of being somebody who knows about Bitcoin and willing to put their money where their mouth is, may be a primary motivation behind retail client investment, under conditions where they are unable to explain how they work. This is not to say that cryptocurrencies do not or will not do what they say they will in the future; rather a comprehensive understanding of cryptocurrencies cannot be assumed by compliance professionals on the part of the retail investor. More specifically:

> *"The average purchasing power parity (PPP)-divided monthly household income per capita in the sample is € 1,116.4, with owners and prospective owners of cryptocurrencies*

8 United States. Congress. Senate. Committee on Agriculture, N. (2009). The role of financial derivatives in the current financial crisis: hearing before the Committee on Agriculture, Nutrition, and Forestry, United States Senate, One Hundred Tenth Congress, second session, pg 75-78 October 14, 2008. Washington: U.S. G.P.O.

9 Jake Frankenfield, *Cryptocurrency*, INVESTOPEDIA (Apr. 7, 2020). https://www.investopedia.com/terms/c/cryptocurrency.asp.

*being poorer by some €140 per month on average. Individuals intending to own cryptocurrencies in the future have some €237 per month lower income, compared to individuals who have heard but do not intend to own cryptocurrencies."*[10]

Furthermore, recent studies reveal that "consumer knowledge about digital currencies is limited, and cash is still king."[11] The paradox is that "the more financially literate candidates were less likely to own cryptocurrencies and they are more likely not to intend to own them in the future."[12] As you can imagine, this is a huge problem for the expansion of the industry. Has there ever been a product so heavily lent on by banks and investors where the more you learn about the product, the less likely you are to want to invest in or use it? The conventional compliance problem is when individuals with specialist expertise, mastery of regulatory loopholes or aspects of a product's application, try to circumvent thorough examination by the compliance analyst or officer. This requires compliance teams to work out what somebody is trying to avoid disclosing and why. In the case of cryptocurrency, it may be the case that many investors know as little as any untrained analyst. The product could be either an inert purchase made on the assumption that it must be a safe bet because of its growing popularity, or a powder keg that requires intensive scrutiny.

In the case of the Abacus scandal, it was only the few at Paulson & Co and Goldman Sachs that knew the full intricacies of the product, and this led to a negative perspective on their success; they took this knowledge and used it to make "short" positions on the product's overall downfall. The study also shows the inverse as it was "the groups with a lower level of knowledge that [were] more open to future adoption."[13] This echoes sentiment felt in the aftermath of the global financial crisis (GFC). Industry reviews, case-law and market research after the crash reveals that only a few people in the market knew what a derivative was, yet they still traded them profitably for some time. But it is not just the problem of traders and their prospective investors. This is a regulatory and policy issue as well, that directly correlates to the treatment and understanding of digital currencies.

"With the growth of various kinds of derivatives in the late 20th Century, there was legal uncertainty as to whether certain derivatives including credit default swaps violated state 'bucket shop' and gambling laws."[14] In fact, the Commodity Futures Modernization Act of 2000 (CFMA) created a safe harbor by pre-empting state and local gaming and 'bucket shop' laws except for general antifraud provisions and exempting certain derivative transaction on commodities and swap agreements including credit default swaps from the Commodity Futures Trading Commission (CFTC) regulation. "As the global economy slows and the risk of corporate default increases [...] recent proposals to regulate CDS

10 See also, Panos. G & Karkkainen. T, p.26.

11 See also, Exton. J.

12 See also, Panos. G & Karkkainen. T, p.30.

13 See also, Exton. J.

14 See also, United States. Congress. Senate. Committee on Agriculture, N. pg 76-78.

markets show limited awareness of the issues," writes Satyajit Das, former banker and treasurer turned consultant and author[15]. If a regulator does not understand the product that they are regulating, then the odds are stacked against the compliance analyst or chief compliance officer, as the likelihood of their knowledge on the subject matter is predetermined by people who lacked awareness of the issues surrounding the CDO and sub-prime mortgage crisis.

Regulators showed a similar lack of awareness and understanding when trying to regulate cryptocurrencies. The SEC deemed virtual currencies to be securities by reason that they are investment contracts and the CFTC has classified them as commodities. Other regulators around the globe followed suit with Canada, Finland and other European countries viewing them as commodities with additional tax measures. Picture a young compliance analyst who has been tasked with covering the commodities trading desks for AML, due-diligence and other regulatory checks. This analyst has come to grips with the standard products that the trading desk usually works with, i.e., gold, oil, energy derivatives or physicals. This analyst has since been told to also conduct checks on cryptocurrencies. That would not require the same level of skills that this person might have been using for this role. They would require training and a complete understanding as to why this has been classified as a commodity. They might even miss a few 'red flag' elements. This is why, despite these products being regulated, lawmakers have not gone far enough. Policymakers have merely opted to box them into existing categories and groups within pre-existing regulation. But they should have examined all of the digital currencies closely and properly understood these products in order to create bespoke legislation that's tailor-made for the industry without ambiguity. Perhaps it should also receive oversight from regulators who actually do understand the product – forming a new body featuring legal financial technology (fintech) and digital currency specialists. Victor N.A. Metallo, assistant professor of Business Law at Montclair State University agrees with this hypothesis, writing:

> *"A need for such an entity is clear when looking at, for example, Ripple Labs's ("Ripple") XRP, a currency designed to work with the existing banking system. Ripple was sued over whether XRP is a security requiring registration with the SEC. Ripple maintains that XRP is a currency, not a security, because a retail purchaser of the currency "does not own rights to the profits or any dividends of the company." Ripple contends all XRP virtual currency have been pre-mined and designed for use by banks as bridge assets and can exist without the company. In light of such lawsuits, Congress should create a separate entity that would classify each virtual currency as a security or commodity and determine which commission, the SEC or CFTC, has oversight."*[16]

---

15 Satyajit Das, *Insight: Credit default swaps and amplified losses*, FINANCIAL TIMES (Apr. 7 2020). https://www.ft.com/content/3ee.5e766-08d7-11de-b8b0-0000779fd2ac.

16 Victor N.A. Metallo, *Are They Commodities or Securities? Virtual Currency Markets – Congress Must Create A New Regulatory Entity*, THE WAKE FOREST L. REV. ONLINE, 44 (Apr. 7, 2020) http://wakeforestlawreview.com/2018/09/are-they-commodities-or-securities-virtual-currency-markets-congress-must-create-a-new-regulatory-entity/.

But Metallo's findings do not go far enough. Virtual currencies should not be classified as any existing financial instrument as they are new entities in the market, requiring their own definition enshrined in legislation. In fact, a recent decision in March 2020 by the Supreme Court in India found that virtual currencies are not commodities.

> *"The Supreme Court after going through various explanations and definitions from different sources, observed that "there is unanimity of opinion among all the regulators and the governments of various countries that though virtual currencies have not acquired the status of legal tender, they nevertheless constitute digital representations of value and that they are capable of functioning as (i) a medium of exchange and/or (ii) a unit of account and/or (iii) a store of value".*[17]

The court investigated the definition of 'currency' as given under various Indian Acts and took into consideration judgments from lower courts to get clarity on the question of whether virtual currencies are just commodities. The judgment stated that the argument of the petitioner, the Internet and Mobile Association of India, that virtual currencies are commodities cannot be accepted. Since it is accepted by some institutions as valid payment for goods and services, "it squarely comes under the purview of the Reserve Bank of India (RBI)." The ruling adds that: "if an intangible property can act under certain circumstances as money (even without faking a currency) then RBI can definitely take note of it and deal with it."[18] The courts essentially denied that these financial instruments were 'commodities', but it did not classify them as 'money' either – rather, they were considered an intangible property that can sometimes get you your groceries. A novel interpretation, but still a bit too ambiguous.

Additionally, to reiterate Metallo's point on XRP, there is not just one type of digital currency. There are several different types of virtual coins and they each come with their own prospective risks. Although this article does not seek to name them all in addition to their inner operations, it will highlight a few below[19]:

- Etherium offers the Ethereum Virtual Machine (EVM) via its platform, a decentralized virtual machine that executes peer-to-peer contracts using a cryptocurrency known as ether.
- Facebook's Libra, a permissioned blockchain digital currency, which will reportedly support both existing government-backed currencies, like the US dollar and the euro, and the Libra token when it is eventually completed and ready to launch.

---

17 Supreme Court of India, Internet and Mobile Association of India (IMAI) v Reserve Bank of India (RBI). Justices: Aniruddha Bose, R F Nariman, J. Ramasubramanian, (Mar. 4 2020) https://main.sci.gov.in/supremecourt/2018/19230/19230_2018_4_1501_21151_Judgement_04-Mar-2020.pdf.

18 See also, SC judgement, IMAI v RBI, 2020.

19 Angela Scott-Briggs, *10 Types of Digital Currencies and how they work*, TECH BULLION (Apr. 7, 2020) https://techbullion.com/10-types-digital-currencies-work/.

- Litecoin is a peer-to-peer cryptocurrency released under the MIT/X11 licence.
- Gemini dollar (GUSD) is an ERC20 stablecoin that allows holders to send and receive US dollars across the Ethereum network and can be exchanged for other cryptocurrencies on other exchanges offering different trading pairs.
- Bitcoin, the infamous digital currency created by the Satoshi Nakamoto, which can be used to buy items locally and electronically.

One crypto-news website's definition on Bitcoin states: "as a new user, you can use Bitcoin without understanding all its technical details. Once you install a Bitcoin wallet on your mobile phone or computer, it will generate the first Bitcoin address and you can generate more whenever you need them."[20] Propagating user consent without distilling the requisite knowledge on them to fully understand the financial instrument in order to make the right decision is a red flag, especially within the compliance industry. But this can only be preserved through the lack of awareness from the top of the chain such as policy makers and regulators, which trickles down to traders and compliance analysts. It is understandable to be a technology consumer and enjoy a company's products without fully understanding how everything goes together (if you broke up my laptop, I would struggle to put it back together), but cryptocurrency is unique in the sense that every user is also a prefigurative retail client. Even if you do not directly invest in the company, to invest in the currency is a similar act, done for similar reasons. To invest in cryptocurrency is to invest with the belief of future utility, of future returns.

Legislators and courts world-wide should reconsider what 'currency' is within this digital age. Although it is well and good that these tools are being regulated, they are not being classified correctly. This only increases the likelihood of a compliance malfunction, fraud or inappropriate trading behavior as the lack of properly defining a financial instrument leaves room for ambiguity. Ambiguity, as shown above, can create risks that should otherwise not exist if someone merely took the time out to understand the product. That knowledge can be distilled all the way to a bank's compliance analyst, who can "tick a box" with confidence when authorizing or prohibiting a certain transaction from taking place.

## III. RECENT DEVELOPEMENTS

Aside from the recent Supreme Court ruling in India determining what is and is not a virtual currency, the story of the digital coin has flourished over the past two years. Various governments and policymakers across the globe have shifted their stance towards authorization of these financial instruments.

The recent UK Budget announcement by Chancellor Rishi Sunak, mentions it "looks forward to the Bank of England's (BoE's) discussion paper on a potential UK central bank

[20] See also, Scott-Briggs, A.

digital currency (CBDC)."[21] In fact, the Bank of Canada, the Bank of England, the Bank of Japan, the Swiss National Bank and the Sweden's central bank, have formed an alliance with the European Central Bank (ECB) and the Bank for International Settlements (BIS), to begin the process of reviewing how a digital currency owned by each country's central bank could come into existence.

In March this year, the US dabbled in the creation of a 'digital dollar' as Congress was putting together the terms of its stimulus package to save the economy from impacts of the coronavirus pandemic. The offer by House Democrats included a forward-looking kind of stimulus: the creation of a 'digital dollar' and the establishment of 'digital dollar wallets.' However, the final version of the economic stimulus package offered by Speaker Nancy Pelosi in the House Democrats, no longer included the US 'digital dollar' proposal.[22]

Russia has also softened its approach towards digital currencies as prime minister Mikhail Mishustin introduced a new bill to the country on 17 March 2020 which creates regulatory sandboxes to test "digital innovation technologies" such as blockchain and cryptocurrency. These products will be exempt from requirements such as mandatory authorised capital, fund reserves and reporting to the central bank, and the standards for the maximum risk per borrower can be cancelled.[23]

Last year was also a big year for governments testing their own digital currencies. China has piloted its digital yuan back in November[24] and the Bahamas begun testing its new digital Sand Dollar in the same year[25]. Although Kenya, Ghana, Nigeria and Mauritius have not formed any plans for a government-backed digital coin, they are also examining the regulation of cryptocurrency as it is still viewed with suspicion and widely viewed as a Ponzi scheme[26]. It was also a year for sanctioned nation states to examine the possibilities of a government backed digital currency as North Korea, Cuba, Venezuela and Iran all

---

21 *HM Treasury and the Rt Hon Rishi Sunak MP*, Budget Speech 2020 (Mar. 11, 2020). https://www.gov.uk/government/speeches/budget-speech-2020.

22 Jason Brett, *Coronavirus Stimulus Offered By House Financial Services Committee Creates New Digital Dollar*, FORBES (Ma. 23, 2020). https://www.forbes.com/sites/jasonbrett/2020/03/23/new-coronavirus-stimulus-bill-introduces-digital-dollar-and-digital-dollar-wallets/#59381f5b4bea.

23 Government House, Moscow, Meeting with deputy prime-ministers (Mar. 16, 2020) http://government.ru/en/news/39161/.

24 Brandon Stewart, *Timeline: China's Digital-Currency (Yuan), Bitcoin And Cryptocurrency*, READBTC (Apr. 7, 2020). https://www.readbtc.com/posts/china-digital-currency-yuan-bitcoin-cryptocurrency-timeline-recent-events.

25 Michael LaVere, *Central Bank of the Bahamas to Launch Its Own Digital Currency 'Sand Dollar'*, CRYPTOGLOBE (Apr. 7, 2020) https://www.cryptoglobe.com/latest/2019/12/central-bank-of-bahamas-launching-sand-dollar-in-exuma/.

26 Jen Stolp, Ashlin Perumall, Emma Selfe, *Blockchain and Cryptocurrency in Africa*, BAKER MCKENZIE (Apr. 7, 2020), https://www.bakermckenzie.com/-/media/files/insight/publications/2019/02/report_blockchainandcryptocurrencyreg_feb2019.pdf.

considered this option in the second half of 2019[27]. In fact, in December 2017, Venezuela's president, Nicolas Maduro, announced the launch of an oil-backed cryptocurrency – the Petro. Maduro made the Petro the "official alternate currency" in the country and reportedly issued 100 million tokens. The Petro was launched in pre-sale in February 2018 and in December, Maduro told state-run media that Venezuela had a schedule for selling oil in Petros during 2019 as part of an effort to bypass channels that involve US dollars.[28]

## IV. ADVANTAGES AND DISADVANTAGES

The above notion of sanctioned countries being able to use cryptocurrencies to assist its citizens comes at an advantage for people who can send and receive money abroad using this tool to pay for their bills and groceries. The advent of cryptocurrency has been a welcome product for these nations as it creates a solution to financial exclusion. Cuba's economy minister, Alejandro Gil Fernandez, said the government was consulting with academics to study the potential use of cryptocurrency for its national and international commercial transactions, while the country's president, Migual Diaz-Canel, announced the plan would raise capital for around one quarter of the population, helping to pay for reforms during a public address on local television[29]. This is a similar approach taken to that of Iran, despite its top legislators being highly dismissive of the product until a conference with business leaders last year. Although this benefits the citizens of these countries under sanctions, it would pose difficult questions for those in the compliance industry working within an institution that adheres to US sanctions.

There are also potential risks for these nations caused by a lack of transparency surrounding digital currencies. As mentioned above, Kenya, Ghana, Nigeria and Mauritius have all been weighing up the potential pros and cons of a virtual currency which is still met with great distrust in the continent. Due to the lack of transparency within these products, it has been easy for scammers and fraudsters to manipulate the system for their advantage, and Africa has been a prime target for these perpetrators.

On a popular BBC podcast, 'The Missing Cryptoqueen'[30], the broadcasting crew discover that Dr. Ruja Ignatova, aka "the Cryptoqueen", had managed to defraud her users for millions of pounds all under the guise of being the next Bitcoin. "Investors often told us that what drew them in initially was the fear that they would miss out on the next big thing. They'd read, with envy, the stories of people striking gold with Bitcoin and thought

---

27 Katherine Kirkpatrick, Christine E. Savage, Russell Johnston, Matthew B. Hanson, *Virtual Currency in Sanctioned Jurisdictions*, KING & SPALDING (Apr 7, 2020), https://www.kslaw.com/news-and-insights/virtual-currency-in-sanctioned-jurisdictions#_edn2.

28 See also, Kilpatrick K, Savage C, Johnston R & Hanson M.

29 Marie Huillet, *Cubans Are Turning to Bitcoin to Access Global Economy: Report*, COINTELEGRAPH, (Sep. 13, 2019).https://cointelegraph.com/news/cubans-are-turning-to-bitcoin-to-access-global-economy-report.

30 Jamie Bartlett, *Cryptoqueen: How this woman scammed the world, then vanished,* BBC (Nov. 24, 2019). https://www.bbc.co.uk/news/stories-50435014.

OneCoin was a second chance,"[31] according to Jamie Bartlett, reporter and podcaster at the BBC. This highlights Baudrillard's point about the sign-value as people wanted to get on the "next big thing" based off hype alone. Even being told to their faces by reporters that they were victims of a proven fraud and that there was an international arrest warrant out for the very person that had convinced them to part with their cash was not enough to dissuade locals. A combination of the anchoring effect, the sunk cost fallacy and the growing political distrust of interloping proscriptive elites lays the ideological groundwork for this type of scheme to operate effectively, acquiring an arguably cult-like following of supporters as emotionally invested in the OneCoin revolution as much as any financial investment made.

Dr. Ignatova managed to launch her OneCoin product in a remote village in Uganda, despite there being publicized revelations in the Western international press flagging it as a potential scam. This illustrates the study by St Andrews that poorer candidates – as those in the Ntangamo region of Uganda were – wanted to invest in something new which can get them out of their current situation. Bartlett wrote: "In Europe, less money was invested in the first six months of 2017 compared to the same period in 2016. But in Africa, the Middle East and the Indian subcontinent, it was the other way around. As the money started drying up in Europe, promoters turned more and more to countries like Uganda."[32] The Financial Conduct Authority (FCA) in the UK issued a warning to investors about the risks OneCoin poses on its website. But how was someone in the Ntangamo region of Uganda supposed to find that out? Western sellers of OneCoin sold the dream to those living in remote towns in the Global South; taking their own lack of transparency and the user's lack of awareness to their advantage. And that was not the only scam that scared off potential CBDC's in the continent.

- Mavrodi Mundial Moneybox (MMM), founded by Sergei Mavrodi, a convicted Russian fraudster, approached the African market and took advantage of Bitcoin's promise to free people from banks and social inequality. "In both Nigeria and Kenya, MMM claimed to be a mutual fund platform where users would contribute their bitcoin to a common funding pool and, in turn, realise 50% returns on their investments." This turned out to be a Ponzi scheme.[33]
- In South Africa, thousands of people lost more than $80 million total in a bitcoin swindle orchestrated by BTC Global, a bitcoin trading company. "The company targeted members of the public and urged them to invest with a promise of 2% interest daily, 14% weekly and 50% monthly. However, after two weeks of operation, the company closed shop and fled with millions in investments."[34]

---

31 See also, Bartlett. J.

32 See also, Bartlett. J.

33 Steven Weru, *Bitcoin Scams In Africa: Their History And How To Avoid Becoming A Victim,* BITCOIN MAGAZINE, (Jul. 19, 2019) https://bitcoinmagazine.com/articles/bitcoin-scams-in-africa-their-history-and-how-to-avoid-becoming-a-victim.

34 See also, Weru S.

- Velox 10 was able to draw in thousands of Kenyans, with some claiming to have lost as much as $30,000 (3,000,000 KES). To join the investment outfit, members were required to pay a registration fee of $100, after which they were promised daily returns of $4,000.[35]

These scams show that it is not a surprise that countries like Nigeria and Kenya are not running into the arms of issuing their own digital currencies so fast, and instead consider enforcing AML protocols first. As lawyers based in King & Spalding suggest, "exchanges, as well as other crypto participants, such as wallet providers, asset managers, and financial institutions, should strengthen AML and CFT frameworks, along with associated KYC procedures, to ensure that cryptocurrency business lines comply."[36]

Scams and a lack of transparency are also not the only issues at hand when considering the use of cryptocurrency. As the world is moving towards more sustainable and environmentally friendly applications and systems, it should be noted that bitcoin "consumes more energy than the entire nation of Switzerland,"[37] according to new estimates published by researchers at the University of Cambridge. The Cambridge Bitcoin Electricity Consumption Index[38] highlights how the global Bitcoin network is consuming more than seven gigwatts of electricity. "Over the course of a year that's equal to around 64 TWh or terawatt hours of energy consumption. That's more than the country of Switzerland uses over the same time period (58 TWh per year), but less than Colombia (68 TWh per year)."[39] With this is in mind, if countries started rolling out large cryptocurrency projects, the energy consumption would only increase, making the world less energy efficient. The European Commission released its Disclosure Regulation, which was published in the EU Official Journal in December 2019. It forms part of a package of measures announced by the European Commission to improve firms' consideration of environmental, social and governance (ESG) issues as part of their decision-making processes. The purpose of the Disclosure Regulation is to achieve more transparency on how financial market participants and advisers consider sustainability risks in their investment decisions and insurance or investment advice. As a compliance manager or broker-dealer, it would be hard to justify these high energy figures on the sustainability disclosure regulations issued by the EU. Sustainability should not just be a buzzword used in conferences or seen as what the youth of today form strikes about. It is something that the financial industry should take seriously as it plays a huge role in adding to pollution, so it should make up for its past mistakes by ensuring ESG matters are properly explored.

---

35 See also, Weru S.

36 See also, Kirkpatrick K, Savage C, Johnston R, Hanson M.

37 James Vincent, *Bitcoin consumes more energy than Switzerland, according to new estimate*, THE VERGE (Jul. 4, 2019). https://www.theverge.com/2019/7/4/20682109/bitcoin-energy-consumption-annual-calculation-cambridge-index-cbeci-country-comparison.

38 Cambridge Bitcoin Electricity Consumption Index (CBECI), Cambridge Centre for Alternative Finance, University of Cambridge Judge Business School.

39 See also, Vincent J.

## V. CONCLUDING REMARKS

If digital coins were going to develop a way of being drastically more energy efficient, hone in on scammers, become more transparent and provide potential users – from employees within trading institutions to your average retail investor – with the requisite knowledge and expertise on the product, then it might have a promising future. But first the industry as a whole must come together to address these issues. The unintelligibility and unfamiliarity of its technological innovations with the layperson, their popularity with first-time retail clients without adequate financial literacy, the prevalence of multiple cryptocurrency scams that exploits the aforementioned intelligibility, and the inherent volatility of products that are bought on the basis of projected brand legitimacy, are all factors that must be addressed within the industry, and known to all compliance analysts engaging with these financial products today. If the current trends in cryptocurrency as a popular financial product continue with a similar makeup of client investors, then we all need to finally know how Plumbuses are made.

CEJ
COMPLIANCE
ELLIANCE
JOURNAL

# NEW SUITS - APPETITE FOR DISRUPTION IN THE LEGAL WORLD

Book review: Michele DeStefano/Guenther Dobrauz (Eds.), Stämpfli Verlag, Bern 2019

Christina-Maria Leeb

## AUTHOR

*Christina-Maria Leeb is a research assistant at HEUSSEN Rechtsanwaltsgesellschaft (practice group IT/IP/Media) in Munich, Germany. Additionally, she acts there as a Digital Business Development Analyst in the "Digitization & Legal Tech" team and holds a PhD in Law (University of Passau, Germany). Her PhD thesis is entitled "Digitalisation, Legal Technology and Innovation - The decisive legal framework and the requirements for a lawyer in the information technology society". Leeb was named "Woman of Legal Tech 2018" by a major commercial law firm, a legal tech company and a thematic blog. In 2019, the Bavarian State Ministry for Digital Affairs included her in the talent program "Bavaria's Women in Digital Professions" as one of 50 women in Bavaria.*

## REVIEWED BOOK

*Michele DeStefano, founder and Content Curator of CEJ, is a Professor of Law at Miami Law and the director and founder of LawWithoutWalls. Guenther Dobrauz-Saldapenna is a Partner with PwC in Zurich, Leader of PwC Legal Switzerland, a member of PwC's Global Legal Leadership Team directing the firm's global legal practice and the firm's Global LegalTech Leader. DeStefano and Dobrauz are editors of the book "New Suits. Appetite for Disruption in the Legal World" published in June 2019. It combines the expertise of 47 (!) authors, many of whom are already proven experts in the worldwide legal tech scene.*

Books related to the digital transformation of law - especially legal tech - have been springing up like mushrooms since about 2018 and continue to do so today.[1] They reflect the great interest of the legal profession in these topics. With *New Suits* a further, particularly impressive volume has been added.

Apart from the well-known American lawyer series, the title recalls the famous works of Richard Susskind, in particular *Tomorrow's Lawyers. An Introduction to your Future* (Second Edit., 2017) and *The End of Lawyers? Rethinking the Nature of Legal Services* (2010). Furthermore, the book already impresses optically with 710 pages and a cover, on which - separated by a blood-red dividing line - on one side a suit-wearer with a tie and on the other side a punk with a Bitcoin button on his leather jacket can be seen. It quickly becomes apparent: In the still very conventional legal book market, signs are yet to be set.

Even the structure is innovative: In Part 1, the question as to why "Lawyers [...] Need New Suits" is posed. Part 2 describes "What New Suits Might Lawyers Need for the Future". Finally, the general question of Part 3 is: "How Will Lawyers Fit into The New Suits of the Future?".

Part 1 consists of eleven single chapters. They describe a colorful bouquet of developments, both with regard to changes in the working methods of legal advisors as well as external factors and new business models. Chapter 1, written by David B Wilkins and María José Esteban Ferrer, starts with Alternative Legal Service Providers. External actors also play a role in Chapter 5, authored by Christoph Küng, where Legal Marketplaces and Platforms are the subject. Karl J Paadam and Priit Martinson devote their important Chapter 10 to developments in the judiciary and administration: *e-Government & e-Justice: Digitizations of Registers, IDs and Justice Procedures*.

One thematic focus is the attorney's working methods and consulting services in selected areas. In Chapter 6, for example, Karl Koller describes the possibilities of using technology in the Practice of Real Estate Transactions, also known as Property Tech (PropTech). Chapters 7 (author: Marc O Morant), 9 (authors: Michael Grupp, Micha-Manuel Bues) and 11 (authors: Christian Öhner, Silke Graf) inform the reader about Gig/Contingent

[1] I have attempted a constantly updated list of all (German and English) legal monographs, manuals and volumes in the field of Legal Tech, E-Government & E-Justice under bitly.com/legaltechdokz.

Workforce Models, Legal Automation and Lawyer Bots. Probably the most important chapter in times of the worldwide outbreak of the corona virus (some people might think of #FlattenTheCurve[2] when looking at the graphic on p. 302) is provided by Eva Maria Baumgartner, without having suspected this at the time of its origin. In Chapter 8 ("Virtual Lawyering - Lawyers In The Cloud"), she provides a *Survival Kit for Lawyers in the Cloud Computing Universe*. Baumgartner quite rightly points out that, "with cloud computing, gathering and distribution of information is excessively enhanced, making it more impactful than any other information technology of our time".[3] One might hope that in practice the necessary steps have already been taken using the Survival Kit before law offices were closed and (as in China and Italy) curfews imposed. In any case, the author sees "lots of room for organizations such as the bars and disciplinary organizations to move towards the cloud and help members to clearly understand requirements to be able to move forward with their clients".[4]

Finally, Part 1 also contains more cross-cutting issues: From Innovation (Chapter 3, author: Michele DeStefano) to *Legal Professionals of the Future* (Chapter 4, author: John Flood) to Corporate Legal Departments, in particular *The Changing Role of General Counsel* (Chapter 2, author: Mari Sako).

The topics from Part 1 are closely interwoven with those from Part 2. The distinction is not readily apparent, but this does not affect the relevance of the chapters. There, legal publishers are also heard as a professional group beyond legal consultancy in Chapter 14, written by Simon Ahammer. In parallel with Chapter 6 (PropTech), David Bundi and Marcel Lötscher each devote their Chapters 18 and 19 to the financial industry (Regulatory Technology - RegTech) and the use of RegTech for supervisory agencies (SupTech).

Part 2 also focuses on new basic technologies in general and the working methods of lawyers in particular. In Chapter 15, Rolf H Weber describes *Smart Contracts and What the Blockchain Has Got to Do with It*. David Fisher and Pierson Grider provide a transfer of the Blockchain topic to the legal sector (outside the regulatory framework) in Chapter 16. Especially worth reading in this context is also Chapter 21, authored by Luis Ackermann.

---

2 *Chow/Abbruzzese*, NBC News, 11/03/2020, https://www.nbcnews.com/science/science-news/what-flatten-curve-chart-shows-how-critical-it-everyone-fight-n1155636.

3 Eva Baumgartner, *Virtual Lawyering—-Lawyers In The Cloud, in:* New Suits 223 (Michele DeStefano, Guenther Dobrauz-Saldapenna, 1st ed. 2019).

4 Eva Baumgartner, *Virtual Lawyering—-Lawyers In The Cloud, in:* New Suits 223 (Michele DeStefano, Guenther Dobrauz-Saldapenna, 1st ed. 2019).

He is concerned with *Artificial Intelligence and Advanced Legal Systems* and provides readers with valuable advice: "Act now, from a position of strength, rethink your IT strategy, free from preconceptions, and be bold enough to not only consider radical change but actually realize it"[5]. Chapters that are particularly practical, as they concern themselves with day-to-day work, are Chapter 17 (authors: Juan Crosby, Mike Rowden, Craig Mckeown, Sebastian Ahrens) concerning eDiscovery, Chapter 20 (author: Antonios Koumbarakis) concerning Legal Research and Chapter 22 (authors: Christian Öhner, Silke Graf) concerning Automated Legal Documents.

Furthermore, two Chapters follow a more general approach. Guenther Dobrauz-Saldapenna and Corsin Derungs focus on *Innovation, Disruption, or Evolution in the Legal World* (Chapter 12). In Chapter 13, Matthias Trummer, Ulf Klebeck and Guenther Dobrauz-Saldapenna cover the *Legal Value Chain*.

Part 3 has a clearer focus, namely on the future-oriented change in job and requirement profiles (mindsets and skillsets) as well as new business models in the law (firm) sector. Under these aspects there are also comments on Legal Procurement (Chapter 25, written by Silvia Hodges Silverstein and Lena Campagna) as well as Restructuring Law (Chapter 26, authored by Tom Braegelmann).

Maurus Schreyvogel opens Part 3 with Chapter 23: *Fix What Ain't Broken (Yet)*. Similar lines are followed by Jordan Urstadt in Chapter 24 (topic: Strategy for Legal Products of Law Firms), Philipp Rosenauer and Steve Hafner in Chapter 27 (topic: Managed Legal Services) and Salvatore Iacangelo in Chapter 30 (topic: Future of Law Firms). Chapters 28, 29, 31 and 32, on the other hand, put more emphasis on the competences and characteristics of the individual. They deal with *Legal Hackers* (authors: Jameson Dempsey, Lauren Mack, Phil Weiss*), New Jobs in an Old Profession* (authors: Noah Waisberg, Will Pangborn), Collaboration and Leadership (author: Michele DeStefano) and - last but not least - Diversity (author: Maria Leistner).

The fact that the book deals with diversity in the legal industry (and what this topic has to do with a lack of innovation and of young talents, too) is exemplary for the far-sighted and outstandingly innovative approach. Often enough it is still wrongly anchored in people's minds: Diversity is not just about gender. Leistner also makes this clear and refers

5 Luis Ackermann, *Artificial -Intelligence and Advanced Legal Systems, in:* New Suits 492 (Michele DeStefano, Guenther Dobrauz-Saldapenna, 1st ed. 2019).

above all to race and age.[6] She convincingly points out that technological changes will assist in attracting more diverse lawyers to teams, "creating the environment that helps them drive: an environment that is not based on selling hours and *presenteeism*, but value adding, with advice being able to be provided 'on the go' and through advanced methods of communication".[7] I look forward to these changes and to such an important chapter being placed further ahead in a new edition of the book.

Overall, a must-read for all those – academics and practitioners alike – who are concerned with the future of legal advice and want to be provided with an "international, multicultural map of the legal jungle (...) by putting together the voices of legal thought-leaders from around the world"[8]. The readers can expect a wide range of topics full of high-quality articles. Comprehensive and fundamental articles provide the necessary basis of knowledge. Thematically more specific articles and particularly beneficial international aspects lead to even the "advanced" legal techies getting their money's worth. After reading this, the legal professionals should get even more excited about fitting their *New Suits*.

6 Maria Leistner, *The Importance of Diversity, in:* New Suits 658 (Michele DeStefano, Guenther Dobrauz-Saldapenna, 1st ed. 2019).

7 Maria Leistner, *The Importance of Diversity, in:* New Suits 666 (Michele DeStefano, Guenther Dobrauz-Saldapenna, 1st ed. 2019).

8 Michele DeStefano & Guenther Dobrauz-Saldapenna, *Curators' Foreword in:* New Suits 8 (Michele DeStefano, Guenther Dobrauz-Saldapenna, 1st ed. 2019).

CEJ
COMPLIANCE
ELLIANCE
JOURNAL

# BOOK REVIEW THE CLIENT-CENTERED LAW FIRM: HOW TO SUCCEED IN AN EXPERIENCE-DRIVEN WORLD

Theresa Albert

## AUTHOR

*Theresa Albert is an academic assistant in the Legal Reports – Defense Proceedings office of Prof. Hendrik Schneider in Wiesbaden, Germany, and studied law at the Goethe University in Frankfurt am Main. The focus of her interests lies in the field of the internationalization and Europeanization of law and the effect of innovations on the legal services market.*

Jack Newton, the author of the work, is the CEO and co-founder of Clio, the largest cloud-based practice management platform for attorneys and other legal practitioners, which is based in Canada. Newton is regarded as a pioneer in this area and uses his experience to resolve security, ethical and data protection issues in connection with cloud computing for the legal community and, in particular, the legal consultancy professions. He is an internationally recognized author and speaker. For those reasons alone, the work "The Client-Centered Law Firm: How to Succeed in an Experience-Driven World", which appeared in January 2020, deserves particular attention.

Newton is not the only person to address the subject of how legal firms can cast off their old apparel and adapt to a modern world characterized by speed, technology and digitization. Over the last three years, in particular, the pressure to change as a result of legal tech and digitization in general has become an ever expanding topic and has been tackled by several authors. In addition to Newton, for example, Michele DeStefano in her work "Legal Upheaval"[1], published in 2018, and Michele DeStefano and Guenther Dobrauz-Saldapenna in their collection of essays "New Suits: Appetite for Disruption in the Legal World" (2019) have focused on this topic and on the impact of legal tech and digitization.[2] The latter work also identifies issues of gender and diversity as drivers of innovation.

Newton gives a very practical insight into the modern legal practice and a guide with ideas on how to create a "client-centered" practice. The book runs to 267 pages and is divided into three parts, which can be summarized by the questions: "What is a 'client-centered' legal practice?", "Why is it important to be 'client-centered'?" and "How does a 'client-centered' legal practice function?".

In the first part, Newton explains why the legal market has changed and why it makes sense to pursue a client-centered approach in an experience-oriented world. In the process, comparisons are made between legal practices and legal practitioners and other customer-focused companies, such as Starbucks, Uber and AirBnB. In this way, Newton shows that, although there are different expectations of legal practices than of the companies mentioned, legal practitioners and, in particular, attorneys find themselves at a watershed where they have to concentrate not only on professionalism and legal competence in the narrower sense, but also on changing consumer and client requirements. He mentions the change in client attitude, the different approach of potential clients when looking for an attorney and the – at least subliminal – expectations with regard to the consultancy service, which must be fast, personal and, above all, practical. However, client-centered does not mean client-first. Newton uses the latter term to refer to a solution presented on a silver platter, when the client has only ordered a milkshake to go. He talks of overkill of legal information in this connection, which clients struggle to process and

1 See also the review of DeStefano by Schneider: *Legal Upheaval: A Guide to Creativity, Collaboration and Innovation in Law*, CEJ, 4, 2, p. 79 ff. (2018).

2 See also the review of DeStefano & Dobrauz-Saldapenna by Leeb: *New Suits: Appetite for Disruption in the Legal World*, in this issue.

which cannot be applied to their businesses. Client-centered solutions are tailor-made legal solutions, in the implementation of which the client is supported, but which are just as legally robust as other detailed expert reports. The author stresses here how a client-centered legal practice can develop an entirely new dynamism and power, allowing it to begin the process of growing and flourishing again. Newton also says that the experience of the client plays a very important part in this context and that the latter is not just paying for the end product and the legal advice, but also for the experience with the attorney or legal practitioner.

The second part explains what it means to run a client-centered legal practice. Newton identifies five core values (Develop Deep Client Empathy, Practice Attentiveness, Generate Ease with Communication, Demand Effortless Experiences and Create Clients for Life) and a client-centered mentality, all of which are constructive here. This is not only explained theoretically, but also developed according to a plan that illustrates the various stages that the client goes through, from the contact search through to the solution to the problem and payment of the bill. Development of a deep empathy is of crucial importance for a client-centered firm in this context.

In the final part, Newton provides the reader with a tool kit for implementing a sustainable change to a client-centered legal practice. He explains how processes and tools can be used effectively and how the team can be encouraged to adopt a client-centered mentality. He also gives tips on how to measure success and handle feedback from clients. This final step puts the wheels of success in motion and is the driver for internal efficiency and growth of the client base, making those wheels turn ever faster.

The book gives a very good and detailed overview of what client-centered means and how it can be implemented. In doing so, it consistently and very clearly highlights the two complementary perspectives on one problem of the client and the service provider. As every firm has a slightly different set of priorities and focuses on different points, strategic factors are placed in the foreground, rather than concrete ways of addressing clients in the form of a guide to acquisition. The author also has empathy for his own target audience: attorneys are always under personal pressure and are expected to make the impossible possible. This pressure is too much for most people and is a source of stress and burn-out. Although the book cannot neutralize that pressure, it takes the reader on a very enjoyable journey in showing how to deal with and possibly reduce it.

It does not matter what professional role the reader plays (from secretary to partner, from a big law firm to a specialist boutique practice) or how long they have been working there. What is important is a willingness to embrace change and to take this step oneself. That is one of the most important pieces of advice that the book has given me personally. I have identified points which we have already dealt with intuitively in a “client-centered” and thus correct way, as Newton sees it, and at the same time I can see other ways of optimizing this approach. Newton’s work provides motivation to move in that direction. His explanations are authentic and colorful, and they inspire self-analysis and reconsideration. You simply have to be prepared to think a little outside of the box in which you are put even as a student.

In conclusion, this book is definitely worth reading for anyone who is involved with the future of legal tech and client-centered legal practices and is looking for inspiration and ideas. It does not matter what part they play – or would like to play – in the overall scheme of things, the key is a willingness to change in some way.