GLOBAL FORUM ON DATA PROTECTION AND NATIONAL SECURITY
REPORT

Prepared by Hermann Knott and Martin Winkler, Andersen, Cologne

8th Additional Volume of the Journal of ***Swiss Chinese Law Review***
ISSN 2673-5407, September 2020

GLOBAL FORUM ON DATA PROTECTION AND NATIONAL SECURITY

Prepared by Hermann Knott and Martin Winkler, Andersen, Cologne

8th Additional Volume of the Journal of Swiss Chinese Law Review
ISSN 2673-5407, September 2020

Report on the Global Forum on Data Protection and National Security (Online), organized by the Swiss Chinese Law Association (SCLA) on August 28, 2020, 13:00 - 15:35 CEST

Prepared by Hermann Knott and Martin Winkler, Andersen, Cologne

1. Agenda

13.00-13.10 CET Time
Welcome Remarks by Swiss Chinese Law Association (Tianze Zhang)

13.10-13.25 CET Time
Compliance of the States and Federal law on Data Protection in US (Alfred j. Saikali)

13.25-13.40 CET Time
Navigating the Increasingly Important and Complicated Regulatory Hurdles of Data Protection & Privacy and Cybersecurity in China (Jianmin Dai)

13.45-14.00 CET Time
Impact of Data Protection laws on M&A (Amrit Mehta)

14.00-14.10 CET Time
Break

14.10-14.25 CET Time
Data Protection and Litigation – An African Case Study (Godson Uochukwu)

14.25-14.40 CET Time
Geopolitics Discrimination in the Global Enforcement of the Sanctions (Philip Hackett Q.C)

14.40-14.55 CET Time
Data Protection at the Global Supply Chains (Şafak Herdem)

14.55-15.15 CET Time
Panel 1 Discussion: Tiktok Case Debates (Saravanan Dhandapani and Ian Wang)

15.15-15.35 CET Time
Panel 2 Discussion: Tracking Coronavirus: big data and the challenge to privacy (Margareth d'Avila Bendayan)

2. Speakers and Experts

2.1. Speakers

Alfred j. Saikali (USA), Chair, Privacy and Date Security Practice at Shook, Hardy & Bacon
Jianmin Dai (China), Partner at Dentons
Philip Hackett Q.C (UK), Barrister at the 36 Group
Şafak Herdem (Turkey), Managing Partner at IR Global
Godson Ugochukwu (Nigeria), Partner at Fortess Solicitors
Amrit Mehta (India), Partner at Majmudar & Partners

2.2. Experts

Margareth d'Avila Bendayan (Switzerland & Israel), De Jure Cabinet de Conseil Juridique
Ian Wang (China), Partner at Deheng
Saravanan Dhandapani (India), Chairman of CNICA

2.3 Chief Reporter

Dr. Hermann Knott, Partner at Andersen, Cologne, Germany
Hareth Ghalaini, Andersen, Cologne, Germany

3. Welcome Remarks from Swiss Chinese Law Association

Mr. Tianze Zhang first welcomed the speakers and participants. He then introduced the subject of the SCLA Global Online Forum and of the 8th SCLA Global Online Forum in particular: In the framework of the Global Online Forum, global challenges of the past months shall be identified and discussed and solutions shall be debated and exchanged.
Data protection is not only a privacy issue, it is also a national security issue. Nevertheless, current political debates focus exclusively on the privacy of data. The relevance of data protection and the need for controlling privacy will further increase. Moreover, the Data Protection issue is a complicated issue, connected with other issues such as the global supply chain.

Mr. Tianze Zhang pointed out that it is a productive forum and therefore also encouraged discussion during the Forum and afterwards.

He then gave a brief introduction of the SCLA.

The SCLA has two main values: The first one is to create a global community, voice and vision of Asian and European lawyers. Hereby a transparent, collaborated and integrated legal world is promoted by reducing the cultural barriers between the countries to understand each other.
The second is to form a global voice of the legal community in the international decision process

The SCLA has 130 members from 13 countries and regions. The members are part of different industries, e.g. the legal industry, international organizations, professional industries and academics.

Moreover, the SCLA coordinates the publication of the Swiss Chinese Law Review which was published in its second edition in August 2020. Mr. Tianze Zhang encouraged the participants to submit ideas they would like to express to the journal. By this, law firms can be entered into the Chinese market and to other international lawyers as the journal is published online and offline, in Chinese and English.

With the forums, the SCLA aims to create a peaceful future by introducing lawyers to each other so that they understand and trust each other and eliminate prejudices. The members shall exchange their experiences from different countries and different sectors.

In August, the SCLA aligned a meeting platform where members can meet, discuss and exchange and also share PowerPoints for example. Virtual meeting rooms can be secured by a password. The meeting platform is accessible under meet.sin.scla.org.

4. Compliance of the States and Federal laws on Data Protection in US

4.1. The US-legislation as a two-layered system

Mr. Alfred j. Saikali started his presentation by explaining that the system of privacy law in the US is a layered one, consisting of two, the federal system and the state system. This means that if a company wants to operate in a certain state it has to observe the federal law which everybody in the USA has to observe and the state law of the specific state the company wants to operate in. The standards in the different states are not consistent, some are more progressive than others. Therefore, the states are considered ‘laboratories’ for law. The Congress observes what works and what

does not work with the different state laws and then may make a state law a federal law because the state law is successful or there is a need for this law on the federal level.

Each state has a Data Breach Notification (DBN) law. A company has the obligation to inform the affected individuals in case there is a data breach that affects personal information. But each DBN law may be different e.g. in the definition of "Personal Information", the time limit for information of the affected individuals in case of a breach can be different or in the requirement to notify the state regulatory authorities in case of such breach. These differences may cause complications as a company has to comply with all applicable regulation. The question of the applicable law depends on where the data subject resides. For this reason, more than one DBN may be applicable to a single company, e.g. when it is a e-commerce company with customers all over the USA.

4.2. The states as laboratories for law

Several states are trying new and different regulations in privacy. For example, California has one of the strictest privacy laws (California Consumer Privacy Act, CCPA). Compared to Europe, Mr. Alfred j. Saikali sees the USA ahead in the area of data security law because, for example, obligations for data breach notifications exist for mor than 15 years and therefore there is experience in its implementation and familiarity with the processes, time frames and requirements. Nevertheless he does not see the USA ahead of Europe in terms of privacy as the legislation in the USA does not provide for the same scope of rights of the affected data subject towards the company as those granted by the GDPR, e.g. the right to access to personal information owned by a company or be forgotten.

Mr. Alfred j. Saikali observes a trend that other states start adopting similar laws to the CCPA or consider adopting such laws. As that trend spread, the federal government could adopt a federal law based on the CCPA.

4.3. Biometric Privacy Law

Another aspect of data protection in the USA is the biometric privacy law. In this context, the Biometric Information Privacy Act exists in Illinois since 2008. It obliges anyone who collects biometric information (e.g. scanning of fingerprints, eyes, face) on somebody in Illinois to give notice to the data subject that this information is collected and to obtain its written consent. In case of not complying, the collector of the data may be sued for USD 1.000 per violation. Two to three years ago, over 500 of such lawsuits have been filed against different companies doing business in Illinois, seeking millions of Dollars.

Mr. Alfred j. Saikali considers the data protection system in the US to be rather reactive than proactive, meaning that it responds to concerns rather than acting proactive and giving data subjects rights as GDPR does, which is a negative aspect.

4.4. Use of civil lawsuits and regulatory enforcement actions

In case of data breach, companies are often sued by transaction lawyers with the argument the companies were negligent in failing to secure information and to adopt reasonable security safeguards that would have protected the information and therefore the individual data subject whose information was compromised shall be compensated. Due to the US civil lawsuit system, each affected data subject would receive a compensation of perhaps USD 5-10 whereas the lawyers who

filed the lawsuit will value the USD 10 for the thousands of people they were representing and take 1/3 of that amount as remuneration, amounting to millions of dollars in contrast to the compensation of the single affected data subject.

4.5. Privacy Notices on websites

There are only sometimes laws requiring such a privacy notice. Nevertheless, information in the Privacy Notices must be correct and complete, otherwise the company may be sued for fraud, negligent misrepresentation. Therefore, companies have to be accurate in their Privacy Policy and disclose what they are doing with the personal data and how they are sharing and using personal information.

4.6. Questions

- Mr. Tianze Zhang: What would be the relevant law for a decision to ban TikTok in the US?

Mr. Alfred j. Saikali feels it was rather an issue of xenophobia, the fear of the foreign, fear of the outside. The fear is that TikTok is collecting Personal Data from US-residents and probably not disclosing everything it is collecting or sharing. On the other hand, US-companies such as Facebook may collect Personal Data and use it the same way TikTok may do. The difference is that TikTok is a China-based company and the concern from a security perspective is what the Chinese government could potentially do with the information collected.

- Mr. Lawrence Ohineme: Is it foreseeable that in the future there will be a unanimous law on data protection like in the EU?

Mr. Alfred j. Saikali thinks that this will not be the case. The main reasons are that the Congress (Democrats and Republicans) cannot decide on whether people should be able to sue in case of violation of the law. The second disputed question is whether the law shall be enforced by the state regulatory authorities or another organization/authority. The third controversial issue is what standard shall the federal law apply? The standard in California may be lowered by a federal law whereas the standard in other states may be raised. This response may have to be corrected if the democrats obtain a sufficient majority in the senate in the coming election.

- Mr. Godson Ugochukwu: It is a balancing act for the companies to comply with the different scopes of information duties and other obligations under the different state laws. How do they manage to fulfill them?

Mr. Alfred j. Saikali handles this issue with his clients by taking the strictest law applying to the respective client as benchmark and considering this law as the client's personal federal law, complying with it in all states it is operating.

5. Navigating the Increasingly Important and Complicated Regulatory Hurdles of Data Protection & Privacy and Cybersecurity in China

5.1. Legal Framework

Mr. Ken Dai first introduced the Legal Framework of Cybersecurity. China announced the National Cybersecurity Strategy on 27th December 2016. The Legal Framework is quite complex in China. There are different Laws like the E-commerce Law or Encryption Law. Furthermore, there is more

and more Soft Law in China, so called Standards. They are not legally binding, however, in practice the authority may reference to the standard. Like in the US there are Sectoral Rules, e.g. Guidelines for Governance of the Data of Banking Financial Institutions or Administrative Regulations on Human Genetic Resources.

5.2. Enforcement Authorities

There is no single Data Protection Authority in China (DPA). Instead there are many competing regulators. For example, there are

- Central Cyberspace Affairs Commission
- Ministry of Public security
- State Administration for Market Regulation
- Ministry of Industry and Information Technology
- and Sectoral Regulators like the Chinese Banking and Insurance Regulatory Commission.

5.3. Legal Consequences

In China there are different Liabilities. On the one hand there are Administrative Liabilities. They contain corporate Liabilities and Individual Liabilities.
The Fines in China are rather low with RMB 1 Million. These fines apply to Business Liability as well as Individual Liability. However, there are further sanctions for businesses than just the fines. For example, the business license may be revoked, or the business can get suspended for a long time. For the Individual it may have an impact on critical positions.
On the other hand, there are Civil Liabilities. This involves the Cessation of the tortious act, the Compensation for losses, the Restoration of the reputation and Apologies. Compared to the U.S. the Liability is soft as there is no cross-action or triple damage regarding data-protection.

Finally, there is the Criminal Liability. There is a climax in criminal sanctions for the breach of data protection and cybersecurity.

5.4. Regulatory Hurdles

Mr. Ken Dai addresses the Regulatory Hurdles. One of the Hurdles is Article 37 of the Cybersecurity Law. If any undertaking falls into the scope of critical information infrastructure operator (CII Operator), all personal information and important data needs to be stored in China. Important Data is Data, that is closely related to national security, economic development, and public interest. Therefore, one has to do a security assessment. That means one has to assess the determination, whether one belongs to the CII Operator. Secondly, if one falls under this scope it is a challenging job for multinational to identify and determine the scope of important data.

It is the first time that the U.S. government has come to the WTO to make a complaint arguing that compliance with this Law is a hurdle for multinationals. Mr. Ken Dai then gave some orientation on the notion of a Critical Information Infrastructure (“CII”) Operator. Accordingly, a critical Information Infrastructure Operator is someone who operates networks or systems that involve for example energy, finance, transportation, water utilities, healthcare, education or social security. And there is also a catch-all provision.

Another Regulatory Hurdle is the VPN (Virtual Private Network). There are more and more enforcement cases in relation to VPN. The possible punishment may be the Cessation of international connection, a warning, fines, or the confiscation of illegal gains. Traditionally, multinationals use the VPN quite frequently to gain access to google, facebook, twitter internally.

5.5. Looking forward

There is new legislation in the Pipeline. The Personal Information Protection Law may be a Chinese version of the GDPR and is going to be released in the next years. Mr. Ken Dai names the Data Security Law and compares it to the CLOUD ACT, that will probably be introduced early next year. There are also supporting Regulations on how to deal with Security Assessment for Cross-border Transfer of Personal Information and how to regulate the Security Protection of Critical Information Infrastructure.

Regarding the Enforcement Development the Special Inspection on App Privacy is ongoing the purpose of which is to control whether the App operator is illegally collecting information. Also, a regulatory action on multi-level protection of information system security is expected.
There is also sectoral regulation ongoing in relation to the Central Bank of China, the Health Commission and the Ministry of HR and social security.

5.6. Discussion

- Mr. Mike Muha: What are the requirements to transfer data over China to the U.S.?

Before he addresses the inquiry, he reminds of the regulatory approach in China: It is crucial whether the company in question is a critical Information Infrastructure ("CII") Operator.

He suggested following framework:

a. What is the nature of the company (e.g. high tech, fast consumer)?

b. What is the position of employee information? It may be identified as personal information as well as important information

c. How can this information potentially be used in other jurisdictions? There is also a blocking statute in China

- Mrs. Margareth d'Avila Bendayan: Is China attending special guarantees from the other countries for the exchange of information like in Europe?

No, because there are no bilateral treaties. Maybe in the future China enters bilateral or multilateral treaties to open more.

- Mr. Godson Ugochukwu:
  - Multiple enforcement authorities – Are there conflicting regulating requirements?

Not conflicted but competing. One must deal with the requirements equally.

  - Does this have any impact on the principle of ease of doing business in China?

Issue of the Tik Tok Cases later in the forum

  - Would cloud storage constitute cross border transfer in China?

Firstly, it is important if the cloud service has the license to provide such service in China. Secondly you have to figure out if the company belongs to the CII Operator

and if the data is allowed to transfer out of China. To resolve such issues, most companies have their local partner in China.

6. Impact of Data Protection laws on M&A

Mr. Amrit Mehta started his presentation by explaining that India is probably the 2nd largest country in the world having maximum smartphone users. As more and more people are working from home, India is on the way to (further) digitalization.

6.1. Current data protection regime in India

The current data protection regime in India is not very detailed and comprehensive. In the year 2000, the Ministry of Communications and Information Technology came up with the Information Technology Act, 2000 (IT Act). The scope of the relevant rules under the IT Act, i.e., the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI rules) was further clarified by a press note issued by the Ministry of Communications and Information technology in 2011.

The SPDI rules have as their main objective to protect sensitive personal data or information (SPDI), which is defined under the SPDI rules. However, SPDI rules only cover such data or information which is exchanged in an electronic form and protects neither data received in a verbal or written form, nor data of juridical persons.

Confidentiality is not codified in India as no specific law protects trade secrets or confidential information. For this reason, confidentiality obligations are usually contractually agreed between the parties. Independent of this, courts have granted injunctions to protect confidential information on the principles of equity and common law. Affected parties are granted temporary or permanent injunctions to protect the information in addition to damages and other contractual remedies the parties may have agreed on in the contract.

6.2. Proposed Data Protection Law in India

As the current law is not very robust and comprehensive, after the coming into force of GDPR in 2018, the Indian government is proposing to enact and fast-tracking a new Personal Data Protection Bill (Data Bill) to protect personal data of individuals. It is not clear when the Data Bill will be enacted and in what form.

The Data Bill is likely to increase compliance and infrastructure costs from a data processing perspective. The Data Bill proposes to implement sanctions in the form of huge monetary penalties. Moreover, based on the GDPR, the Data Bill suggests implementing definitions of various terms such as data processor and data principal. Indian companies operating will be affected by the new law as well as overseas entities if they have a connection in terms of processing data belonging to natural persons.

The Data Bill distinguishes between three categories of data: personal information, sensitive personal information and critical personal data. These terms will be defined by the Government and specific requirements and rules will be established for each type of data. Pursuant to the Data Bill, a copy of any data processed will have to be stored on a server or data centre located in India. Moreover, cross-border transmission of data will only be permitted by way of intra-group schemes

approved by the data protection authority, which is to be established under the proposed law. In addition, periodic data audits will be mandatory and records of data processing and data protection impact assessments will have to be maintained. Also, the processing of critical personal data outside India will be prohibited.

Data processing will be allowed in special cases without the approval of the data protection authority if such personal data is processed for any reasonable purpose, including, but not limited to, M&A.

The scope of exemption with regard to M&A is currently unclear. It needs to be defined which data may be processed in which stage of the transaction (due diligence, signing, closing, post-closing integration).

6.3. Key issues in M&A Transactions

6.3.1. Due Diligence

Given the fact that no codified regime or law on confidentiality exists in India, non-disclosure and confidentiality agreements are signed between the parties to ensure that relevant information is adequately protected. Under the current law, targets in data centric industries such as financial services, information technology related services and pharmaceuticals must be investigated for compliance with the SPDI obligations under the current legal regime. It is also to be ensured that sharing of information during the due diligence is in compliance with applicable law. For this purpose, virtual data rooms with limited access and monitoring rights can be used or redacted or anonymized documents can be shared.

Post enactment of the Data Bill, the involved parties will need to ensure compliance with incremental obligations provided therein which may result in higher costs.

6.3.2. Documentation

Representations and warranties need to be included in the transaction documents, comprehensive indemnities need to be considered. In case of breach, indemnities shall be specified in the transaction documents.

6.3.3. Post-transaction integration of acquirer and target

When it comes to the integration of the target into the company of the purchaser, sharing of employee records and other personal data will need to be protected under the terms of the transaction documents. Data sharing with affiliates of the parties should be monitored and protected through appropriate clauses.

6.4. Recent Ban imposed in India

On June 29, 2020, the Indian Government imposed a temporary ban on 59 Chinese apps (among others, TikTok) as it considered these apps to be prejudicial to the sovereignty and integrity of India, its defense, the security of state and the public order. These considerations were based on the assumption that a lot of these Chinese companies were data mining and thus having a lot of personal and sensitive data of Indian users. The Indian government has issued a questionnaire to the affected companies for them to make their representations on the items in question.

The ban was imposed in exercise of the government's powers under the IT Act and the Information Technology (Procedure and Safeguards for Blocking of Access of Information by Public) Rules, 2009 (Blocking Rules). When banning these apps, the acting authority was likely in line with its competences.

6.5. Questions

- Mr. John Popolizio: Is there a consideration of SME vs. larger companies and how is this playing up with the different legislation which may come into force in India?
Mr. Amrit Mehta expects the Indian government to make exemptions for SME and Start-ups, probably for a limited period of 3-4 years. The Data Bill includes a provision allowing the government to determine exemptions and in view of the special demands a start-up faces, an initial period could be regarded as a kind of pilot period during which facilitations can be applied.

- Mr. Tianze Zhang: What will be the changes in the course of the law compared to the current legislation?
Mr. Parshant Philips shared his opinion that he expects the new law to be comparable to the GDPR. Nevertheless, there will be a few deviations, e.g. the definition of personal data, the right to data access or data portability.

- Mr. Xiiaobing Tang (WTO): Concerning the e-commerce the members of the WTO are discussing, has there been a ban on the basis of the Blocking rules before the recent ban on 59 Chinese apps mentioned before?
Mr. Amrit Mehta answered that this was the first ban based on these regulations, neither temporary nor for an indefinite period.

7. Data Protection and Litigation – An African Case Study

7.1. Overview

When introducing the topic, Mr. Godson Uochukwu described that the data protection in Africa has gained a lot from GDPR. This fact is a positive one for companies interested in operating in Africa as they are mostly faced with regulations that are well-known to them. When complying with the GDPR-regulations, companies mostly also comply with the respective national data protection regulations.

In addition to various national legislation on data protection by African countries, on 27. June 2014 the African Union adopted the Convention on Cybersecurity and Personal Data Protection (Malabu Convention). This treaty was signed by 14 states and ratified by 8 out of 55 member states. To become enforceable, it needs to be ratified by at least 15 countries. As of March 2020, 23 African countries have comprehensive data legislation in place. These regulations are heavily influenced by the GDPR.

7.2. Data Protection in Nigeria

Nigeria's government agency NITDA was created in 2001 and is charged with data protection and to this end to develop guidelines for electronic governance and monitor the use of electronic data interchange. On this basis, NITDA issued the Nigerian Data Protection Regulation (NDPR) in 2019. It is Nigeria's reaction to the GDPR and the most significant and comprehensive data protection

regulation in Nigeria. NDPR is not an act of the Nigerian National Assembly but considered as subsidiary legislation according to the Nigerian hierarchy of regulations. However, given the space that it occupies, it is as effective as any other law.

The NDPR defines data broadly as any personal information, insofar as the data subject is identifiable. It applies to natural persons resident in Nigeria and natural persons of Nigerian descent residing outside Nigeria and all organizations processing the personal data of such individuals. Personal data may be processed (a) with the consent of the data subject, (b) for the performance of a contract to which the data subject is party, (c) for compliance with a legal obligation, (d) to protect the vital interest of the data subject, and € for the performance of a task carried out in the public interest. Moreover, the NDPR creates Data Subject Rights which did not exist before, such as the requirement of opt-in/out of data collection for marketing purposes, right to erasure/to be forgotten or the right to correct, restrict or withdraw consent to own data collection. In case of default, a fine of up to 2% of the annual gross revenue may be imposed.

The NITDA has carried out various enforcement actions since its inception thus a sensitization for available rights arose.

7.3. Data Protection in South Africa

In South Africa, the relevant law for data protection is the Protection of Personal Information Act (POPIA) which was passed in 2013 and is principally based on the EU Data Protection Directive 95/46/EC. POPIA comes into force on a rolling basis. Substantive provisions came into force on 1. July 2020, certain provisions will take effect on 30 June 2021. POPIA is largely similar to NDPR in its content. Though, in contrast to GDPR, POPIA applies to natural persons as well as juristic persons processing personal information in South Africa. In case of default for which strict liability is provided, up to 10 years imprisonment or administrative fines up to the amount equivalent to approx. USD 580,000 can be imposed as penalty.

7.4. Data Protection in Kenya

Regulations for data protection in Kenya are laid down in the Data Protection Act (DPA) which came into force in November 2019. Like NITDA and POPIA, DPA is also heavily influenced by GDPR. DPA applies to data controllers and processors established or resident in or outside Kenya, so long as they process personal data while in Kenya or of data subjects located in Kenya. DPA establishes conditions for data processing which has to be lawful, fair, transparent and for a specified purpose.

To ensure the compliance with the Act by the obligated individuals, DPA provides for a Data Protection Commissioner. The processing of Sensitive Data, such as data concerning the data subject's race, health status, belief, genetic/biometric data, sex or sexual orientation etc. is restricted by DPA.

In case of default, up to 10 years imprisonment and/or fines up to the amount equivalent to approx. USD 46,100 can be imposed as penalty

7.5. Challenges and recommendations

Africa is a communal society and therefore, privacy rights in the meaning of the provisions described above can be described as a foreign, but not an unknown, concept.

As enforcement proceedings in Africa are not fast but quite expensive, enforcement of data privacy breaches remains weak, particularly in terms of the complaint resolution role of the public authorities. Therefore, the competent authorities should provide for an alternative way offering the affected data subjects a faster and cheaper way to enforce their rights under the data protection regulations. Along with that, a much greater awareness of personal data and privacy rights by the affected data subjects is needed. To drive this forward, robust government measures are needed.

7.6. Questions

- Margareth d'Avila Bendayan: Can we expect in the nearer future a common and global legislation concerning the protection of data by the African countries?

Mr. Godson Ugochukwu answered that theoretically the answer is yes, once the respective countries have ratified the treaty. But when it comes to enforcement, national differences have a huge impact so that the same provisions may have different effect in reality depending on the country the decision or judgment shall be enforced.

8. GDPR in the UK after Brexit and Geopolitical Discrimination in the Enforcement of regulatory Sanctions

8.1. GDPR in the UK after Brexit

8.1.1. GDPR: Regulation (EU) 2016/679

GDPR is seen by the European Union as the gold standard of data protection and is quite widely respected all over the world.
From the 1st January 2021 the UK will have its own independent system of regulation. The question is what the difference will be compared to the European Law.
The main difference will be the enforcement. The enforcement of regulatory matters is as much a matter of geopolitics as law.

8.1.2. Data transfer to third countries

Mr. Philip Hackett introduces an English case in the English Court of Appeal called Johnson and the Secretary of the State for the Home Department of 2020 as example of how the court approaches enforcement of data protection.
An individual had been deported to Jamaica out of country and appealed the deportation out of country. The hearing took place in Jamaica. The UK government tried to send all the material about him, and he objected, arguing that the material were data and that sending the material for the hearing was an infringement of his rights. The court confirmed GDPR as domestic UK Law but argued, that the hearing took place in the UK embassy in Jamaica, so there was no transportation of data to another country. Sending the material was furthermore necessary and proportionate and justified and compliant to the Human Rights Act.
The law requires an adequacy decision. That is the adequacy of a data protection law of the receiving country. One of the problems on this behalf will be, that for example a country like Jamaica will be economically challenged, it is not going to have the resources or the refined governmental systems. The question is if it will ever be able to comply on an adequacy decision as receiving country under EU Law which will now become UK Law. This highlights the potential discriminatory effects. Mr. Hackett states that for that reason the court had to take this artificial way out, saying that there was no transportation because the British embassy is not Jamaica.

8.1.3. Third Party Adequacy Decision

Mr. Hackett thinks that this part is highly controversial, as the Third-Party Adequacy Decision states a standard, that the Third Party must raise to. The EU Court has decided that the U.S. does not meet the standard. EU Law has to be matched in every aspect, not just in Data Protection. This leads to the problem, that friendly or unfriendly countries are being treated differently. For example, Nigeria is very close to the UK for historical reasons as they adapted the Common Law, the legal system is very close to the UK. But African countries are most likely not to meet the high standards of the EU Law. As conclusion Mr. Hackett states, that there will have to be flexibility in enforcement.

8.1.4. The Privacy Shield

The US system has the US Privacy Shield regime. The court of justice of the EU said, that this regime is not valid for the purposes of transfer of data. The reasoning behind that is the lack of limitation on the power conferred to the implementation of certain US government surveillance programs. Maybe this can be compared to the actions against TikTok.
The court also felt there was a lack of sufficient guarantees for individuals and non-US individuals and a lack of actual data subject rights before the US courts against the US government and therefore lack of equivalence with the EU law. There is still the chance of transatlantic data transfer under the standard contractual clauses. Mr. Hackett is sure that the solution to this topic has to be a political one.

8.1.5. Enforcement: Public Authorities

Although it was thought that there would be a lot of actions and class actions similar to those in the US. In terms of general damages, the English Courts do not come near the sort of amounts that are awarded in the US especially by juries. The regulatory body (Commissioners office) might be one of the reasons why there has not been much enforcement because they are not traditionally a prosecuting body. The government bodies do not employ many lawyers specializing in these sorts of arias. They nearly try to proceed based on a deal. At the moment there are some big cases going on against big companies. But apart from that there is not much action.

8.1.6. Enforcement: Civil Litigation

The Civil Litigation is not a big source of Litigation and there is no sign, that it is going to be different in the future.

8.1.7. Does the BREXIT make any difference?

In theory it should not make any difference. The GDPR is retained as domestic law.

8.1.8. Post BREXIT

The immediate issue is the flotation of data between the EU and the UK as there is currently no adequacy decision in place. The controversy will be in enforcement going forward. For example, France often has a different forum policy to the UK. France will deal with countries in a sympathetic and collaborative manner that the UK will regard as being in breach of international laws. Mr. Hackett can imagine France making substantial concessions to Third Party countries to give them a favorable adequacy decision. Despite the UK would not give those countries a favorable adequacy decision. The problem is that the flow between the UK and France would be dependent not only on the situation in UK or France but also on the relationship between UK or France between third party Countries.

8.2. Geopolitical discrimination in enforcement of regulatory sanction

Mr. Hackett shortly referred to geopolitical discrimination. Classic examples for Discrimination of non-EU and non-UK citizens are money laundering and tax investigation for example the freezing of bank accounts. In Mr. Hackett's experience there is several Chinese citizens in the UK whose bank accounts have been frozen. The reason for that is in many cases, that these Chinese citizens move their money in legal but unusual ways.

Sanctions on the other hand are dealt with at a government level. The sanction policy is well administered. The sanction departments see their job as representing the UK's interests and keeping the UK international.

Mr. Hackett raised the question, „How did the UK get the money to Iran?", speaking of 1.3 billion Pounds as settlement for illegal imposition of sanctions, as transferring this kind of money is in breach of US unilateral sanctions.

8.2.1. Sanctions: Politics or Law

Mr. Hackett says that Sanctions are mainly political. There is no unilateral basis for US Iran Sanctions. It relies on enforcement.

8.2.2. UK Sanctions after Brexit.

He thinks the UK sanctions will remain the same after the Brexit unless the UK is under the influence of the US.
Will the UK adopt the EU "Blocking Regulation" 2271/96, that states that not every US law has to be enforced. The UK does not have this Regulation domestically, it is part of EU Law.

He then shorty asked: Will INSTEX succeed and continue? INSTEX is a system that the EU has for trading with Iran, so one can avoid being extradited to be tried in New York.

8.3. Questions

- Mr. Mike Muha: Is the privacy shield dead under the UK Data Protection Act?

Mr. Hackett: No. That decision is an EU-decision. Starting 1st January 2021, the UK has to make its own decisions. Mr. Hackett can imagine a decision in favor of the US.

- Mr. Godson Ugochukwu asked: Concerning Art. 48 of the GDPR: Do you consider this provision problematic given the regard third country requests for information to the EU?

Mr. Hackett: EU has implicated that once the BREXIT is finalized the UK would become treated as a third country Do you also see such a problem for the UK is there a redemptive treaty that could resolve this issue on the Art. 48?
Mr. Hackett thinks that the UK and the EU will find an agreement. The problems that arise from third party requests after an agreement between the UK and the EU will be negotiated. But there will be conflicting decisions made. The UK will follow its own course but will be in alignment with the EU in principal.

9. Data Protection at the Global Supply Chains ab 2:43:00

In the beginning of his presentation Mr. Şafak Herdem introduces the regulatory Landscape. He differentiated between “National Security” and “Technology”. Both fields have the Data Protection and Privacy Matters in common.
From the business perspective there are Data Related Business and Non-Data Related Business. Data Protection and Supply Chains are a common topic of both parts.
To understand where these issues are in a global supply chain, one needs to understand the rule makers. The policy-based approach was more an optional implementation.
There are other technological developments like artificial intelligence, big data, analytics, networking, IoT. Data Protection has a high impact on these Data-intensive businesses.
It is not only about the data collection and storage, but also about the processing and trade of data. Mobility issues and medical devices are based on electronical or sensitive technologies, that are collecting and processing data. The Data collected may be personal or commercial but at the end of the day these are data.

9.1. Digital Supply Chain Management

9.1.1. Backbones of Digital Supply Chain Management

Regarding the Data-Driving businesses the questions arising are:

- Is it about something computational or sensory?
- Is the business about a product, a device, a system or a platform?
- If you are providing a Data Related Service, is this service for
    - Infrastructure
    - Platform
    - Software or
    - Business processes

9.1.2. Questions regarding Personal Data Based Process

From a global perspective trading has change under the landscape of data. Technology and technology revolution are globally discussed. In the Data-Driving Business the Questions regarding Personal Data Based Processes are:

- Who owns the technology?
- Who is the beneficiary?
- Who has the control?

9.1.3. Questions regarding the Origin of Data in Business

- Are all associated items and activities only in your jurisdiction?
- Does it contain any foreign origin item?
- Does the technology or the device bundle or commingle with other controlled technology of other jurisdictions?

9.1.4. What is the purpose of the data?

It is not a question of one field only. The main question is not, where the Data is made in, but who the Data is made by.

Discussed issues are: Data used for

- National Security
- Military Purposes
- Civil Purposes
- Dual-Use Purposes
- Controlled Technology

9.2. Data Protection and Privacy Matters

Concerning personal Data there are five questions arising:

- Whose data is actually concerned and associated
- Quality and Quantity: Storage and Profiling
- Who will design and engineer the digital supply chain for privacy matters?
- What about the Apps: are there default privacy settings?
- Soft Law and self-responsibility principles: Restrictions to use in certain areas/ times

9.3. Product related Matters

- Is the product for commercial purposes, who is the end-user?
- What happens if there is malfunction?
- Is the Data accurate?
- What are the Compatibility, Manufacturing and Labelling requirements in supply chain?
- What happens if the device fails or is damaged by human?
- What if the Data is manipulated in any way?

The Made in China Program 2025 and the U.S: Export Control Reform & Foreign Investment Review Modernization Act both involve processing of personal data.

Mr. Herdem points out that Personal Data exists in various kinds of technology and can be used for both Civilian and Military purposes. For example, Advanced Surveillance Technologies are used in “Face ID” or in Enhanced army goggles.

Finally, Mr. Herdem shortly introduces a Case Study on HUAWEI and the TikTok Case and states that the whole journey began with claims on personal data concerns.

10. Panel 1 Discussion: Tiktok Case Debates

Opening the panel discussions, Mr. Tianze Zhang introduced Mr. Hermann Knott as the moderator and gave him the word.

10.1. Reflections on TikTok Case and Data Privacy as National Security

To start Panel 1, Mr. Knott gave the word to Mr. Ian Wang. Mr. Wang first introduced the participants to the TikTok case and its background.

10.1.1. Background of the TikTok Case

TikTok is a Chinese video-sharing social networking app launched in 2017 having more than 1 billion users worldwide. Since February 2019, the UK Information Commissioner's Office (ICO) launched

an investigation on TikTok and its data collection, but not on the data transfer. In June 2020, India banned TikTok along with 59 Chinese phone apps. The US government enforced TikTok to sell its shares to an US-based company. Moreover, a Presidential Order was issued abandoning all transactions with TikTok.

These proceedings against TikTok in both India and the USA are based on National Security Concerns due to the collection of personal data of local citizens and their transfer to China. Mr. Wang considers the underlying issue to be a political rather than a juridical one.

10.1.2. Does the Chinese Government Have Access to the Data?

In China, four provisions exist that may grant the Chinese Government access to the personal data TikTok collected and still collect. These provisions are laid down in the National Intelligence Act of 2017, the Cyber Security Law of 2017, and the National Security law of 2015. Moreover, a draft of the Data Security Law dated 2020 exists that deals with approval obligations when collecting data and cooperation obligations.

10.1.3. How TikTok Case Would Impact on Chinese Legislation?

Due to the circumstance that foreign governments take discriminatory enforcement actions against TikTok, the Chinese government may pass a law in response to the TikTok case. The draft of the Data Security Law dated 2020 will probably be passed. In view of the TikTok case, there might be some amendments of the draft.

10.1.4. Balance between Data Flow and National Security/Privacy Concerns

To open the floor for the discussion, Mr. Wang asked the questions in the room if the national security/privacy concerns are real or just a pretext. If they were a pretext, would more “walls” be built between the nation borders and would this have a negative impact on digital economy/tech industries due to constrained cross-border data flow? If they were real concerns, could more proper measures be implemented to mitigate these concerns?

10.2. View on the TikTok Case from an Indian Perspective

In the beginning of his presentation, Mr. Saravanan Dhandapani pointed out that two things are dangerous, becoming more popular and becoming too beautiful. This happened in the TikTok case. It is a very popular app all around the world. He warns that some of the users who have no self-control loose themselves and are addicted to this app and that innocent children and women become victims unknowingly.

In 2019, a lawsuit was filed against TikTok India to direct the Indian government to take actions against TikTok India to ban the application, which was degrading culture, increasing pornography, containing disturbing content and including danger of addiction. In April 2019 an Indian court has granted an interim order prohibiting the download of the TikTok app and the medias telecasting the TikTok videos. TikTok has filed an appeal before the Supreme Court of India to revoke the interim order. However, the Indian Supreme Court has relegated the case to the court of first instance. TikTok moderates the content using the artificial intelligence moderation vision at a first level and human moderation in the next three levels. And even then, there is a grieving’s-officer who can be directed. The court lifted the prohibition by cancelling the fact that the Indian Information Technology Act of 2002 and the Rules of Regulation are comprehensive enough to address the problem.

The court also considered the Sections of the Information Technology Act and the Information Technology procedural safeguards for blocking for access of information made public Rules 2009 under the Information Technology Intermediates Guideline Rules 2011. It also observed that there is an adequate machinery under the Act and Rules to deal with the intermediaries who fail to respond or act to complaints. TikTok has undertaken that it does an extensive due diligence in accordance to the requirements of Information Technology Act 2000 and the Rules thereunder. Thereby ensuring the safety and security of all his users.

Under these circumstances there was a border tension between India and China. In June 2020 by invoking on the Information Technology Act the government of India has banned 58 mobile applications, including TikTok, on the ground that those applications are against integrity, security and public orders. Meanwhile there was a lot of complaints about the Data and breach of privacy on TikTok and other applications. The computer emergency response team of India has also received many representations of Cities regarding Security of Data and breach of privacy effecting public order issues. Based on this the government of India has issued the interim prohibition TikTok and other applications tried to convince the Committee. The Committee can make a recommendation based on which the government may lift the ban or not.

10.3. Questions and Comments

Mr. Hermann Knott opened the round of questions and discussions and pointed out that from both sides, China and India, the reasons for the handling of TikTok seem not only to be national security but also health issues due to the danger of addiction TikTok contains.

- Mr. Ian Fry described his concerns about the impact of the decisions of non-western countries and that politics are involved in these decisions. To him, India seems to be caught in a triangle.

  Mr. Tianze Zhang wanted to know how global companies handle the requests for data transfer by a government.

  Mr. Ian Fry replied, taking the relations between Australia and the USA as example, that no technology is involved in these decisions but an agreement between the two countries is signed so that the transfer is a pure political decision. Mr. Fry cannot predict what would be the result if this case would be taken to court in Australia or another jurisdiction.

- Mr. Knott: Is it realistic that data can be collected as it is reproached to TikTok or is it unlikely from a technical or Chinese legal point of view?

  Mr. Ian Wang replied that according to the respective CIA report it is possible that the Chinese government had access to those data but it cannot be proven that they actually had. Under the Chinese law, the Chinese government may ask any company to cooperate for reasons of national security. It needs to be mentioned that the US-Cloud Act grants the US-authorities the same powers as the Chinese law does.

  Even if the Chinese government had abused its power to gain access to this information it needs to be evaluated if the total ban of TikTok is an appropriate measure.

- Mr. Alfred j. Saikali mentioned the importance of distinguishing between the legal and political issues with respect to TikTok. From a legal perspective the concern may arise whether TikTok sufficiently discloses all of the information they have, how they use and how they store this information. The political aspect on the other hand it needs to be pointed out

that other similar companies based in the USA are not treated the same way as TikTok (e.g. their sale to a US-entity to do business in the USA). TikTok is treated a different way because it is a Chinese-based company. Under another US-President in the recent history TikTok would not have been treated this way.

- Mr. Tianze Zhang: How is the due process procedure in India as the Indian Data Protection Law seems to give the Indian authorities a lot of authority or powers to ban respective software?

Mr. Saravanan Dhandapani replied that the ban of TikTok was only an interim ban, not a permanent one. Based on the representation of the respective company following the questions the competent authority raises, the authority recommends how to operate in the future to comply with applicable law. Not only TikTok but all social media platforms hold information about their users. The interim ban provides the opportunity to make submissions and to give explanations about how their system works and how they protect their users etc. The Committee than makes a recommendation to the government whether this application can be operated in India. On this ground the government of India my take a position.

REPORTER's COMMENT

New regulations regarding technology exports were promulgated by China's Ministry of Commerce just on the Friday of our Forum, August 28, 2020, introducing the requirement of government approval for the export of certain technologies, part of which are restrictions for "personalized information recommendations services based on data analysis." TikTok is built on algorithms that analyze user behavior to push personalized content. Since then it seems to have become remarkably quieter around this transaction. Does this mean that the government and Mr. Zhang Yiming who appeared to have favored a sale of the US operations (but why?) have not been working in the same direction?

11. Panel 2 Discussion: Tracking Coronavirus: big data and the challenge to privacy

11.1. Tracking Covid-19 with new technologies

In the early stages of the battle against Covid-19, several governments thought that the new technologies would help in the fight against the virus. Therefore, several governments developed different apps for mobile devices:

In China, an app named Alipay Health Code was developed determining if the user of the app is in risk of infection with Covid-19 based on the trips he has made.
Germany has developed an app to measure the spread of Covid-19 in the population. The user voluntarily wears a connected watch or bracelet that records the vital signs emitted by the person and likely to be altered in the event of respiratory illness.
For Israel, the Shin Bet, an internal intelligence service generally focused on counter-terrorism activities, has developed an app allowing to geolocate the mobile phones of people possibly infected by Covid-19.
The respective app in Switzerland allows the tracking of Covid-19 infection chains through the movement data collected by mobile phones. In case a person is tested positive on Covid-19, it can anonymously activate the notification service. Depending on the date of the first symptoms, all users of the app would be then informed if they had been in contact with this person during the potentially infectious period.

11.2. Privacy or health

Taking Israel and Switzerland as examples, the use of these apps was very controversial. In Israel, different organizations and politicians were strongly opposed to this measure. In Switzerland, a citizen's committee has launched a referendum against the app.

The core of the debates is about the balance between privacy and public health interest. Article 8 of the European Convention on Human Rights (ECHR) protects the individual's privacy. No interference by a public authority shall occur unless the interference is in compliance with the law and necessary for the purpose of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health and morals or to protect the rights and freedom of others. The scope of application of Article 8 ECHR is broad. Among others, it protects against geolocalization as well as against the collection of private information. Exceptions from this could be notably for the protection of health.

11.3. The need for a legal basis

If an exception from Article 8 ECHR shall be granted, it has to be founded on a legal basis which needs to be clear and understandable to all citizens.

The Swiss government had the opinion that no legal basis for the use of the Covid-19-app was required because sufficient instruments already existed, and the use of the app was voluntarily. Nevertheless, the competent parliamentary committee recommended to establish a legal basis by the parliament. Following this recommendation, the Swiss Law on Epidemics was adopted.

Israel as well launched a bill regulating the use of the use of the Covid-19-app after the Supreme Court issued a respective ultimatum to the government. The Israeli parliament approved the bill for a limited period of time. Pursuant to this law, the Shin bet will not be in contact with any patient or any person who has been in close contact with the patient and will not be responsible for monitoring the isolation of the individuals concerned.

11.4. Questions and Comments

- Mr. Tianze Zhang pointed out that cultural differences affect the solution of each government and on the reaction of the people to the implementation of an app in connection with the battle against Covid-19 and its spread as well as to the balance between privacy and public health interest the respective people accept.

- Mr. Mike Muka described the reaction to such apps in the USA. Some do not mind giving out personal information for the benefit of the health of the community. Another group of people, especially conservative right, who see this question as a question of individual rights vs. the government and they do not want to be dictated by the government as to how they should behave. This reaction is not necessarily based on the opinion that this information would not be useful for the battle against Covid-19 but rather that the government is spying on them. Moreover, they are concerned that the information collected may be used by the government for purposes other than fighting Covid-19.

- Mr. Hermann Knott described the situation in Germany regarding privacy rights and Covid-19. He reported on a planned demonstration in Berlin against measures in connection with Covid-19 which was first forbidden by the local government of the State of Berlin and then permitted by emergency order of the competent administrative court. This aspect shows the conflict between the basic rights to privacy and public interests.

12. Closing remarks

Finally, Mr. Hermann Knott invited Mr. Tianze Zhang to make his closing remarks: Mr. Zhang thanked the panelists and the audience for this great Forum and discussion and invited the participants to share ideas and articles with the SCLA and the colleagues to keep in touch. He also announced the upcoming forum, which will take place on the last Friday in September.

Mr. Zhang then gave the last word to Mr. Knott who also thanked all participants and underlined that the forum was shaped by the speakers, the panelists and all participants. In this forum, the participants looked at a very broad range on actual and pressing issues related to data protection and not only the substance was very wide but also most of the regions of the world were covered and different issues in different continents were addressed.