情報通信法学研究会通信法分科会（令和３年度第２回）

中国における個人情報保護法
―中国における個人情報保護法制と、経済安全保障の文脈下におけるクラウドサービスにおけるデータの適切な運用に関する法的示唆等を含む―

桃尾・松尾・難波法律事務所　　弁護士・北京大学博士（法学）
松尾剛行

2021年12月20日

MOMO-O, MATSUO & NAMBA
桃尾・松尾・難波法律事務所

目次

引用元については発表用原稿（構成員限り）をご参照ください。

はじめに

CONTENTS

中国において初めての個人情報保護法典が本年制定・施行された。同法に加え、サイバーセキュリティー法（ネットワーク安全法）、データセキュリティー法等の関連法制度を踏まえた個人情報保護法制について日本や欧州の法制度との表面上の類似性及びその背景思想における重大な相違等について概説した上で、特に経済安全保障の文脈下におけるクラウドサービスにおけるデータの適切な運用に関する法的示唆等の観点から説明したい。

第２　中国の個人情報に関する制度概要

１　個人情報保護法

　これまで、中国において、「個人情報保護法典」は「制定する」、「制定する」と繰り返し言われながらも制定されない時期が長く続いていた。しかし、2021年8月20日に、第十三期全国人民代表大会常務委員会第30回会議の審議を経て、中国個人情報保護法が正式に可決成立し、同法は公布され、同年11月1日に施行された。

https://detail.tmall.com/item.htm?spm=a230r.1.14.142.82dc19ebVc6wrw&id=654558177577&ns=1&abbucket=5

第２　中国の個人情報に関する制度概要

２　サイバーセキュリティー法（ネットワーク安全法）

サイバーセキュリティー法は2016年に制定された。一連の個人情報に関する法制度の中では比較的早期に制定されている。同法はネットワーク空間の主権並びに国の安全及び社会の公共の利益を保つこと等を目的としている（1条）。同法はネットワーク上にある情報を規制対象としている。そこで、個人情報であっても、ネットワーク上で管理されていない個人情報、例えば紙ベースやスタンドアロンの個人情報は同法の適用対象とはならない。しかし、ネットワーク上の個人情報については適用対象となるところ、同法は国内保存義務（データローカリゼーション規制）を導入したことで広く知られている（第37条）　。なお、同法76条5号は、「個人情報」を、電子的またはその他の方式により記録され、単独またはその他の情報と組み合わせて自然人の個人の身元を識別することができる各種情報をいう、と定義した。

第２　中国の個人情報に関する制度概要

３　データセキュリティー法（データ安全法）

　データセキュリティー法（2021年6月10日公布、2021年9月1日施行）は、データ処理活動を規範化し、データセキュリティーを保障し、データの開発利用の促進、個人組織の権利利益の保護そして、国家主権、国家安全及び国家発展の利益を維持することを目的としている。同法の規制はデータという観点からのものであり、その対象は個人データに限られないものの、個人データを含む。そこで、中国の個人情報保護を理解する上で重要である。

https://detail.tmall.com/item.htm?spm=a230r.1.14.137.a14e47f94lNMcf&id=649590989315&ns=1&abbucket=5

第２　中国の個人情報に関する制度概要

４　その他民法典等における個人情報保護

中国では民事法に個人情報を保護する規定が設けられてきたところ、中国の民法典（2020年5月28日公布、2021年1月1日施行）は、個人情報を定義しており、その中では、サイバーセキュリティー法における個人情報の定義とほぼ同様の内容が定められている。すなわち、同法1034条2項では、「個人情報」とは、電子的またはその他の方式により記録され、単独またはその他の情報と組み合わせて特定の自然人を識別することができる各種情報をいう、とされている。そして、その中には、自然人の氏名、生年月日、身分証番号、個人の生物識別情報、住所、電話番号、電子メール、追跡情報等が含まれるが、これらに限らない、ともされている。また、民法典では、個人情報の概念のほか、個人情報の取扱過程における本人の権利（たとえば、閲覧、コピー、異議の提出など）及び個人情報取扱業者の義務（適法・正当・必要という原則の遵守、本人同意の取得、取扱ルール・目的・方法・範囲の提示、適切な保管義務など）をさらに明確にした。

なお、中国の電子商取引法（2018年8月31日公布、2019年1月1日施行）等においても、個人情報の保護に関する条項が定められている。

参考スライド

サイバーセキュリティー法76条5号	民法1034条2項
「個人情報」とは、電子的またはその他の方式により記録され、単独またはその他の情報と組み合わせて自然人の個人の身元を識別することができる各種情報をいう。	「個人情報」とは、電子的またはその他の方式により記録され、単独またはその他の情報と組み合わせて特定の自然人を識別することができる各種情報をいう。その中には、自然人の氏名、生年月日、身分証番号、個人の生物識別情報、住所、電話番号、電子メール、追跡情報等が含まれるが、これらに限らない。

第２　中国の個人情報に関する制度概要

５　国家安全法、国家情報法（国家諜報法）、反テロリズム法、暗号法等の国家安全（情報）法制

憲法は中国の根本法である。憲法の国家安全に関する規定には、政治的安全、経済的安全、軍事的安全が含まれ、公民、事業体の具体的義務も含まれている。

国家安全法（2015年7月1日公布、同日施行）は、2015年改正を経て公布、施行された。同法により、政治安全、軍事安全、経済安全、資源・エネルギー安全、食糧安全、文化安全、ネットワークと情報安全などを含む全方位の安全枠組である**「全体的な国家安全観」**が確立された。国家安全法は中国の国家安全法体系における基礎法である。同法第四章第2節には情報の安全について規定されている。国は、統一的に集中し、迅速に反応し、正確かつ効率的に、スムーズに稼働する諜報情報収集、研究・判断及び利用制度を健全化し、諜報情報業務の協調メカニズムを確立し、諜報情報の適時収集、正確な研究・判断、効果的な使用及び共有を実現すると規定されている（同法51条）。

第２　中国の個人情報に関する制度概要

５　国家安全法、国家情報法（国家諜報法）、反テロリズム法、暗号法等の国家安全（情報）法制

反テロリズム法（2015年12月27日公布、2018年4月27日改正、同日施行）は、テロリズム活動を防止し、処罰すること等を目的としている（同法1条）。テロリズム情報の伝播を防止するために、電気通信業務経営者、インターネットサービスプロバイダは、法律、行政法規の規定に基づき、サイバーセキュリティ、情報内容監督制度及びセキュリティ技術の防止措置を実行し、テロリズム、過激主義内容を含む情報の伝播を防止しなければならず、テロリズム、過激主義の内容を含む情報を発見した後、直ちに伝送を停止し、関連記録を保存し、関連情報を削除し、かつ公安機関又は関連部門に報告しなければならないとされている（同法19条1項）。また、電気通信とインターネット企業は本人確認義務を履行すべき旨が明確に規定されている。電気通信事業者、インターネットサービスプロバイダは顧客の身分について確認を行わなければならず、身元が不明である又は身元確認の実施を拒否した顧客に対してはサービスを提供してはならないとされる（同法21条）。加えて、反テロリズム法第18条は、電気通信業務経営者、インターネットサービスプロバイダは公安機関、国家安全機関によるテロ活動の調査に技術インターフェースや機密解除などの技術サポートを提供しなければならないと規定している。

第２　中国の個人情報に関する制度概要

５　国家安全法、国家情報法（国家諜報法）、反テロリズム法、暗号法等の国家安全（情報）法制

国家情報（諜報）法（2017年6月27日公布、2018年4月27日改正、同日施行）は、国の情報（諜報）業務を強化し保障し、国の安全と利益を保護することを目的としている（同法1条）。国の情報（諜報）活動は全体的な国家安全観を堅持し、国の重大な政策決定のために参考となる情報を提供し、国の安全に危害を及ぼすリスクの防止と解消のために情報（諜報）のサポートを提供し、国の政権・主権の統一、領土保全、人民の福祉、経済社会の持続可能な発展と国のその他の重大な利益を守るとされている。

第２　中国の個人情報に関する制度概要

５　国家安全法、国家情報法（国家諜報法）、反テロリズム法、暗号法等の国家安全（情報）法制

暗号法（2019年10月26日公布、2020年1月1日施行）は、暗号の応用と管理を規範化し、暗号事業の発展を促進し、ネットワークと情報の安全を保障し、国の安全と社会公共の利益を守り、公民、法人とその他の組織の合法的権益を保護することを目的としている（同法1条）。暗号法では、国が暗号を分類管理することが規定されている。暗号はコア暗号、通常暗号、商用暗号に分けられる（同法6条）。コア暗号、通常暗号は国家秘密情報の保護に用いられ、コア暗号が情報を保護する最高の国家秘密機密レベルは極秘レベルとされ、通常暗号が情報を保護する最高機密レベルは機密レベルとされ、コア暗号、普通暗号は国家秘密に該当する（第7条）。商用暗号は、国の秘密ではない情報を保護するために使用される（第8条）。

第２　中国の個人情報に関する制度概要

６　経済安全保障の文脈を踏まえた制度間の相互関係

国家安全法によって、法律の形式で、「全体的な国家安全観」という考えが確立された。

サイバーセキュリティー法は、インターネット空間の安全を保障するための重要な法的根拠となった。データセキュリティー法は、データ処理活動を規範化した。個人情報保護法は、個人情報が情報セキュリティの重要な内容であることを示している。

このように、中国では、国家安全法、サイバーセキュリティー法、データセキュリティー法、個人情報保護法という4つの主要な法律に基づき、国家安全、サイバー安全、情報安全、データ安全という四つの点に重点を置いて規制している。

第２　中国の個人情報に関する制度概要

６　経済安全保障の文脈を踏まえた制度間の相互関係

<table>
<tr><td>基礎法</td><td colspan="3">国家安全法</td></tr>
<tr><td>一般法</td><td>サイバーセキュリティー法
（2016年）</td><td>個人情報保護法
（2021年）</td><td>データセキュリティー法
（2021年）</td></tr>
<tr><td rowspan="2">行政法規、部門規章</td><td>ネットワーク安全審査弁法（2020年）
個人情報と重要データ国外移転安全評価弁法（パブリックコメント募集案）（2017年）
児童個人情報ネットワーク保護規定（2019年）、
個人情報国外移転安全評価弁法（パブリックコメント募集案）（2019年）、
データ安全管理弁法（パブリックコメント募集案）（2019年5月28日公布）、
ネットワーク安全等級保護条例（パブリックコメント募集案）（2018年）等</td><td></td><td></td></tr>
<tr><td colspan="3">ネットワークデータ安全管理条例（パブリックコメント募集案）（2021年）
データ国外移転安全評価弁法（パブリックコメント募集案）（2021年）</td></tr>
<tr><td>国家基準</td><td>GB/T 39335-2020情報安全技術個人情報安全影響評価ガイドライン（2020年）
GB/T 35273-2020情報安全技術個人情報安全規範（2020年）</td><td></td><td>情報安全技術データ国外移転安全評価ガイドライン（パブリックコメント募集案）（2017年）</td></tr>
</table>

第３　中国個人情報保護法制の特徴－EU等との比較

１ 国内保存義務及び域外移転規制

サイバーセキュリティー法の定めたデータ国内保存義務（データローカリゼーション規制）は有名であるが、個人情報保護法も同様の義務を課している。個人情報保護法40条では、重要情報インフラ運営者及び取扱う個人情報が国家インターネット情報部門の規定する数量に達した個人情報取扱者は、中華人民共和国域内で収集し又は発生した個人情報を域内で保存しなければならないとされている。そして、確かに域外に提供する必要がある場合には、国家インターネット情報部門による安全評価に合格しなければならない。なお、法律、行政法規及び国家インターネット情報部門が安全評価を行わなくて良いと規定する場合には、その規定に従うとされている。

第３　中国個人情報保護法制の特徴－EU等との比較

１ 国内保存規制及び域外移転規制

また、全ての個人情報取扱者に課される一般的な域外移転のルールとしては、本人に必要事項を告知した上での個別的同意を得ること（39条）に加え、以下の4つのいずれかが必要である（38条1項）。

(一)本法第四十条の規定に基づく国家インターネット情報部門による安全評価に合格した場合。

(二)国家インターネット情報部門の規定に基づく専門機構による個人情報保護の認証を得ている場合。

(三)国家インターネット情報部門が制定する標準的契約を域外の移転先と締結し、双方の権利及び義務を約定する場合。

(四)法律、行政法規又は国家インターネット情報部門の規定するその他の条件。

特に3号でGDPRのSCC(標準的契約条項)類似の内容が含まれていることが注目される。既に本年7月には策定作業が開始されたと報道されており、近日中に公表されることが想定されるものの、2021年12月17日時点では公表されていない。

第３　中国個人情報保護法制の特徴－EU等との比較

２　ガバメントアクセスに関する制度

国内保存義務（データローカリゼーション規制）の結果として、政府が民間企業の保有するデータ等に強制的にアクセスすること、すなわち「ガバメントアクセス」が容易となる。もちろん、従来から刑事捜査や刑事手続きの一環としてガバメントアクセスは行われてきた。しかし、近年では、情報機関等によるガバメントアクセスが注目されている。例えば、中国の国家安全法、国家情報法、サイバーセキュリティー法、データセキュリティー法は、ガバメントアクセスを可能とする規定を有する。

- 国家安全法77条に基づき、国の安全に危害を及ぼす活動の手がかり、証拠の提出や、必要な便宜の提供や協力が求められており、同条4号では「公民」一般が協力義務を負う。
- 国家情報法7条1項に基づき、いかなる組織と公民も、法に基づき国家情報活動を支持、協力、連係し、知っている国家情報活動の秘密を守らなければならないとされている。
- サイバーセキュリティー法 28 条に基づき、ネットワークプロバイダは、公安機関及び国の安全機関のため法に基づき国の安全及び犯罪捜査の活動を維持・保護し、技術支援及び協力を提供しなければならないとされている。
- データセキュリティー法35条によれば、国家の安全又は犯罪の捜査のために関連する協力を求められる場合、関連組織および個人は協力しなければならないとされている。

第３　中国個人情報保護法制の特徴－EU等との比較

２　ガバメントアクセスに関する制度

確かに、匿名で行われるサイバー犯罪やネットワーク上の国家安全を脅かす行為に対する対応として、プロバイダ等の支援を受けて行為者の身元を明らかにすること等はどの国でも必要であるといえるだろう。

例えば、日本でもサイバー犯罪対策としてのガバメントアクセスは存在するし、いわゆる捜査関係照会事項によるガバメントアクセスについては議論があり、例えば一般財団法人情報法制研究所（JILIS）捜査関係事項照会問題研究タスクフォースは、「捜査関係事項照会対応ガイドライン」を公表している。*

但し、中国の場合、例えば国家安全法７７条４号が「公民」一般に国家安全への協力義務を設ける等、読み方によってはかなり広範な義務を課していることから、欧米や日本等において懸念が表明されている。

* https://www.jilis.org/proposal/data/sousa_guideline/sousa_guideline_v1.pdf

第３　中国個人情報保護法制の特徴－EU等との比較

３　中国における情報の取扱いルールの特徴

中国個人情報保護法5条～10条は、個人情報の取扱に関し、以下の原則を打ち立てている。

- 合法性・正当性・必要性・信義誠実（5条）
- 取扱目的の明確性と合理性・取扱目的との直接関連性・本人権利利益への影響が最小となる方法・最小範囲の個人情報の収集(6条)
- 公開・透明性・ルールの明示（7条）
- 情報の質の保証（正確性・完全性）（8条）
- 責任・安全確保(9条)
- 法令遵守・国家安全・公共利益保護（10条）

参考スライド

中国個人情報保護法の原則	GDPR
• 合法性・正当性・必要性・信義誠実（5条） • 取扱目的の明確性と合理性・取扱目的との直接関連性・本人権利利益への影響が最小となる方法・最小範囲の個人情報の収集(6条) • 公開・透明性・ルールの明示（7条） • 情報の質の保証（正確性・完全性）（8条） • 責任・安全確保(9条) • 法令遵守・国家安全・公共利益保護（10条）	・適法性、公正性(5条1項(a)) ・目的の限定 (5条1項(b)) ・データの最小化 (5条1項(c)) ・透明性 (5条1項(a)) ・正確性(5条1項(d)) ・完全性及び機密性(5条1項(f)) （・アカウンタビリティ(5条2項)） ・記録保存の制限(5条1項(e))

第３　中国個人情報保護法制の特徴－EU等との比較

３　中国における情報の取扱いルールの特徴

中国個人情報保護法の特徴として、GDPRと類似する、個人情報取扱のための正当化事由が挙げられる、以下の7つの状況がなければ個人情報を取り扱うことができないとした（13条）。

中国個人情報保護法13条	GDPR6条1項
(一)本人の同意を取得している場合。	(a)　データ主体が、一つ又は複数の特定の目的のための自己の個人データの取扱いに関し、同意を与えた場合
(二)本人が当事者の一方となる契約の締結又は履行に必要な場合又は適法に制定された労働規章制度及び適法に締結された集団的契約に基づき人事管理を実施する上で必要な場合。	(b)　データ主体が契約当事者となっている契約の履行のために取扱いが必要となる場合、又は、契約締結の前に、データ主体の要求に際して手段を講ずるために取扱いが必要となる場合
(三)法定の職責又は法定の義務の履行に必要な場合。	(c)管理者が服する法的義務を遵守するために取扱いが必要となる場合
(四)突発的な公衆衛生上の事件に対応し、又は緊急状況下において自然人の生命、健康及び財産の安全の保護のために必要な場合。	(d)　データ主体又は他の自然人の生命に関する利益を保護するために取扱いが必要となる場合
(五)公共の利益のためメディア報道、世論監督等の行為を実施し、合理的範囲内で個人情報を取り扱う場合。	(e)　公共の利益において、又は、管理者に与えられた公的な権限の行使において行われる職務の遂行のために取扱いが必要となる場合
(六)本法の規定に基づき合理的な範囲で本人が自ら公開し又はその他適法に既に公開済みの個人情報を取り扱う場合。	(f)管理者によって、又は、第三者によって求められる正当な利益の目的のために取扱いが必要となる場合。ただし、その利益よりも、個人データの保護を求めるデータ主体の利益並びに基本的な権利及び自由のほうが優先する場合、特に、そのデータ主体が子どもである場合を除く
(七)法律、行政法規の規定するその他の状況。	

第３　中国個人情報保護法制の特徴－EU等との比較

４　域外適用

データが国際的に流動する中、中国においてもネットワーク安全法やデータ安全法等、多くの法令に域外適用を明記する姿勢が見られる。そして、その傾向は個人情報保護法においても見られる。

中国個人情報保護法3条2項は、中国域内の自然人を標的として製品、サービスを提供し、又は中国域内の自然人の行為を分析し評価する場合、個人情報取扱者が中国域内にあるか否かを問わず、中国法の管轄を受けるとする。これはGDPRの域外適用規定に近接している。例えば、日本企業が越境ECを通じて、このような要件を満たす中国域内の自然人の個人情報の取り扱いを行うと、中国個人情報保護法が直接適用される。

参考スライド

中国個人情報保護法3条2項	GDPR3条2項
中華人民共和国の域外において、中華人民共和国域内の自然人の個人情報を取扱う活動が、以下に列挙する状況の1つを具備していれば、本法をも適用する。 (一)域内の自然人に向けて商品又はサービスを提供することを目的としている。 (二)域内の自然人の行為を分析し、評価する。 (三)法律又は行政法規の規定するその他の状況。	取扱活動が (a)「データ主体の支払いが要求されるか否かを問わず、EU域内のデータ主体に対する物品又はサービスの提供」 又は (b)「データ主体の行動がEU域内で行われるものである限り、その行動の監視」と関連する場合、本規則は、EU域内に拠点のない管理者又は処理者によるEU域内のデータ主体の個人データの取扱いに適用される

第３　中国個人情報保護法制の特徴－EU等との比較

５　国家の関与に関する規定

(1) サイバーセキュリティー法

サイバーセキュリティー法はネットワーク空間の主権並びに国の安全及び社会の公共の利益を保つこと等を目的としているところ（1条）、国家の責務として国内外からもたらされるネットワークの安全上のリスク及び脅威をモニタリング、防御、処置が規定されている（5条）。また、全ての個人及び組織を名宛人として、ネットワークの安全を脅かしてはならず、ネットワークを利用して国の安全、栄誉、利益を脅かし、国家政権の転覆及び社会主義制度の転覆を煽動し、国の分裂及び国家統一を破壊することを煽動し、テロリズム及び過激主義を宣揚し、民族に対する憎悪や差別を宣揚し、暴力及びわいせつな情報を流布し、虚偽情報を捏造、拡散して経済の秩序及び社会秩序を撹乱し、他人の名誉、プライバシー、知的財産権その他の適法な権益を侵害する等の活動に従事してはならないとする（12条）。

また、禁止されている情報があれば、プロバイダに送信停止を命じ、中国国外からもたらされた情報については、技術措置及びその他の必要な措置を講じて伝播を遮断するよう関係機関に通知する（50条）。国はネットワークの安全のモニタリング事前警告及び情報通報の制度を確立する（51条）。

第３　中国個人情報保護法制の特徴－EU等との比較

５　国家の関与に関する規定

(2)データの越境移転に関する安全評価

サイバーセキュリティー法第37条は、データ越境移転の制限に関する安全評価制度を規定した。まず、サイバーセキュリティー法は、日本やヨーロッパ流のいわゆる国外移転規制のみを規定する枠組みと異なり、そもそも個人データを取り扱うビジネスを中国で運営する以上は中国で当該データを保管することを義務付ける国内保存義務（データローカリゼーション）を（一定範囲で）求めている。その上で、国内保存義務の適用対象事業者が例外的にデータを越境移転する場合、政府の安全評価を必要とした。

サイバーセキュリティー法第37条と同様に、中国個人情報保護法40条では、重要情報インフラ運営者及び取扱う個人情報が国家インターネット情報部門の規定する数量に達した個人情報取扱者は、中華人民共和国域内で収集し又は発生した個人情報を域内で保存しなければならないとされている。確かに域外に提供する必要がある場合には、国家インターネット情報部門による安全評価に合格しなければならないとされている。

第３　中国個人情報保護法制の特徴－EU等との比較

５　国家の関与に関する規定

(2)データの越境移転に関する安全評価

情報安全技術データ国外移転安全評価ガイドライン（パブリックコメント募集案）3.7条によれば、ネットワーク運営者は、ネットワーク等の方法により、中華人民共和国国内の運営において収集し、発生させた個人情報と重要データを、直接の提供、又は業務の展開、サービス・製品の提供等の方法を通じて、国外の機構、組織又は個人に提供する一回の活動又は連続的活動を指す、とされている。

ただし、サイバーセキュリティー法の法文上、安全評価義務がかかる範囲は比較的狭いように見える。安全評価の主体は、重要情報インフラ運営者に限定し、安全評価対象客体は、個人情報及び重要データに限定されている。これに対し、個人情報保護法は、取扱う個人情報が国家インターネット情報部門の規定する数量に達した個人情報取扱者に拡大した。なお、サイバーセキュリティー法の下位規範である各法令の草案の動き（未施行）についても留意が必要である。

第３　中国個人情報保護法制の特徴－EU等との比較

５　国家の関与に関する規定

(3) 当局の承認・許可

個人情報の取り扱いにつき、当局の許可や承認を得なければならない場合も存在する。例えば、「人間の遺伝データの管理に関する暫定弁法」の第4条及び第11条が政府の許可なくして越境移転することを禁止している。

加えて、データキュリティー法36条は「中華人民共和国関連主管機関の承認を得なければ、国内の組織、個人は中華人民共和国域内に保存されているデータを域外の司法又は法執行機関に提供してはならない」と規定する。これは、外国のガバメントアクセスに対応した規定である。

同様に、個人情報保護法第41条では、国際司法協助又は行政法執行協助のため、中国国外に個人情報を提供する必要がある場合、主管部門に申請し、その許可を得なければならないとする。

第３　中国個人情報保護法制の特徴－EU等との比較

５　国家の関与に関する規定

(4)ネットワーク安全等級保護制度

サイバーセキュリティー法は、ネットワークサービス提供者を含むネットワーク運営者に対して一連のネットワーク運営上の安全保護に関する要求及び義務を規定しており、ネットワーク運営者が国の実施しているネットワーク安全等級保護制度に基づき、そのネットワーク運行安全保護義務を履行するよう要求することが含まれる。したがって、ネットワーク運営者はサイバーセキュリティー法及びネットワーク安全等級保護制度の要求を遵守する必要がある。ネットワーク安全等級保護制度について、企業は、情報安全等級保護管理弁法及び情報セキュリティ技術ネットワーク安全等級保護基本要求（GB/T　22239-2019）に従って、ネットワーク安全等級を認定し、該当する等級に基づいて、安全の共通要求及びクラウドコンピューティング、モバイルインターネット、IoT、工業制御システムなどの安全に関する保護措置を講じる必要がある。

第３　中国個人情報保護法制の特徴－EU等との比較

５　国家の関与に関する規定

(5) まとめ

上記のとおり、中国では、そもそも日本等において政府が関与していないような民間の個人情報の取り扱いに対して関与をしている。

このような政府の関与は、中国政府の個人情報への強い関心、とりわけそれが国家安全に密接に関係しているという考えを反映している。

参考スライド

データ分類・等級保護制度

データ安全法では、国家安全や公共の利益などに与える危害の程度に応じて、データを分類管理する分類・等級区分保護制度が規定されている。国が重要データ保護リストを制定する等、ここでも国家の関与が認められる。

データの分類について、正式な規定はまだ存在しないが、「ネットワークデータ安全管理条例」（パブリックコメント募集案）（2021年11月14日公布）では、　データを一般データ、重要データ、コアデータに分けている。また、データ等級に関する統一的な規定はまだ公表されていないが、一部の分野では既に関連規定が存在している。例えば、工業データ分類・等級別ガイドライン（試行）、証券先物業データ分類・等級別ガイドライン、金融データ安全データ安全等級別ガイドラインは、データ分類等級別の原則、範囲、規則方法、具体的プロセスについて具体的に定めた。

第３　中国個人情報保護法制の特徴－EU等との比較

６　日本企業の中国ビジネスへの影響（クラウド以外）

(1)　自社への適用の確認

中国に子会社がある企業は基本的に中国個人情報保護法が適用されると考えるべきである。しかし、中国に子会社（エンティティ）がないからといって、中国個人情報保護法が無関係と軽信してはならない。域外適用規定が置かれていることから、自社又は自社グループの非中国企業が、中国個人情報保護法の域外適用を受けないかについて確認をすべきである（４参照）。

第３　中国個人情報保護法制の特徴－EU等との比較

６　日本企業の中国ビジネスへの影響（クラウド以外）

(2) 社内規程、プライバシーポリシー等の改訂

個人情報保護法は個人情報取扱ルールを制定し、明示すべきとしているところ、既に日系企業グループであれば、何らかの個人情報取扱ルールが定められているところも多いだろう。しかし、個人情報保護法は様々な面で規律を追加している。例えば本人の権利に関する規律やセンシティブ情報に関する規律、そして自動的意思決定に関する規律等は、従前の法制度や規格・基準に比べるとより完全化され、包括的・網羅的なものとなっている。そこで、社内規程、プライバシーポリシー等の改訂が必要であろう。

第３　中国個人情報保護法制の特徴－EU等との比較

６　日本企業の中国ビジネスへの影響（クラウド以外）

(3) 日本への移転

中国子会社の取り扱う個人情報を日本に移転させる場合、2021年11月1日の個人情報保護法施行日以降は、原則として本人に必要事項を告知した上での個別的同意を得ること（39条）に加え、安全評価、認証、標準的契約等のいずれかが必要である（38条1項各号）。実務上は標準的契約の利用の方向に収斂するのではないかと予想されるものの、標準的契約の策定状況等を注視する必要がある（上記１参照）。

第３　中国個人情報保護法制の特徴－EU等との比較

６　日本企業の中国ビジネスへの影響（クラウド以外）

(4) 最新状況の注視

上記では標準的契約の策定状況への注視の必要性について述べたが、これ以外にも実務を回していく上での細則等が不明確な状況は国家インターネット情報部門の規定について言及されている38条、40条、42条、45条等が存在する。今後とも下位規範制定等に向けた最新状況を注視していかなければならない。

第４　経済安全保障とデータガバナンス

１ 経済安全保障とは

2020年12月の自由民主党の「『経済安全保障戦略』の策定に向けて」は、経済安全保障を「わが国の独立と生存及び繁栄を経済面から確保すること」を定義し、戦略的自律性の確保及び戦略的不可欠性の維持・強化・獲得という考え方を提示した。

また、経済安全保障の重要な内容について、データこそ経済安全保障の要とされ、また、中国の政策の変化に目配りをする必要がある等の指摘がある。

https://www.kantei.go.jp/jp/101_kishida/actions/202111/19kanban.html

第４　経済安全保障とデータガバナンス

２ 経済安全保障とデータガバナンスーLine事件を踏まえて

(1) 経済安全保障の情報分野への影響

2021年12月3日、都内で開催された第１回防衛・経済安全保障シンポジウムでは、岸田総理は、5G基地局、あるいは洋上風力・海底ケーブル、こうした取組の際に、海外企業を通じて、我が国の安全保障に関わる情報が外国に渡るリスクがあるのではないかという問題意識を提起した。情報通信関係では、①ランサムウェア攻撃（ランサムアタック）等の高度なサイバー攻撃を含む情報流出、技術流出、②ガバメントアクセスを背景としたデータガバナンスの問題の２つの問題が重要であるところ、①は興味深い反面、本発表のテーマとずれるので、本発表では②を中心に検討する。

第４　経済安全保障とデータガバナンス

２ 経済安全保障とデータガバナンスーLine事件を踏まえて

(2) データガバナンスとは

データガバナンスは多義的であり、公的データに対するガバナンスという側面で議論するものも多いものの、民間企業との関係では、DMBOKI(データマネジメント知識体系ガイド)は、データガバナンスをデータマネジメントを統制するための活動とし、「DX 時代における 企業のプライバシーガバナンスガイドブック ver1.1」は、企業のプライバシーガバナンスとは、プライバシー問題の適切な リスク管理と信頼の確保による企業価値の向上に向け、経営者が積極的にプラ イバシー問題への取組にコミットし、組織全体でプライバシー問題に取り組むための体制を構築し、それを機能させることとし、経営者が取り組むべき三要件として、①ガバナンスに係る姿勢の明文化、②保護責任者の指名及び③取組に対するリソースの投入を挙げた。

https://data-viz-lab.com/datagovernance

第４　経済安全保障とデータガバナンス
２ 経済安全保障とデータガバナンスーLine事件を踏まえて

(2) データガバナンスとは

定義には様々なものがあるが、各企業のガバナンスの対象として、従来人や資産等が念頭に置かれてきたが、データの重要性が高まることで、単に個別のデータを管理することそのものを超えて、組織としてその管理の枠組みをどのように作り、どう統制・統御を効かせていくかに注目が集まっており、特に経営者の責任が問題とされている、ということと概ね総括することができるだろう。そして上記の経済安全保障やガバメントアクセスが重要な問題となっている状況においては、そのような観点を踏まえたデータガバナンスが重要である。

参考スライド

「デジタルトランスフォーメーションの河を渡る ～DX推進指標診断後のアプローチ～」は、データを資産としてマネジメントし、あらゆるレベルでデータマネジメント活動を導くための原理原則、ポリシー、プロセス、フレームワーク、メトリクス、監督を提供するとする。ファイブセーフモデルのデータガバナンスフレームワークではSafe Project、Safe People、Safe Data、Safe SettingおよびSafe Outputを重視し、Jill Dyche´=Evan Levy,Customer Data Integration: Reaching a Single Version of the Truthは「企業のデータ活用戦略、目標、ポリシーを確立するための組織的な枠組み」とする。
なお、公的データへのガバナンスのニュアンスがあるものの、EUの「REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
on European data governance (Data Governance Act)案」は、パブリックセクターにおけるデータの再利用の条件、データ共有サービスの通知・監督フレームワーク、利他的目的で公表されるデータの収集と処理を行うエンティティーの任意的登録フレームワークとする
(https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=71222)

第４　経済安全保障とデータガバナンス
２ 経済安全保障とデータガバナンスーLine事件を踏まえて

(3)Line事件に見る経済安全保障とデータガバナンス

LINEにおける海外個人情報アクセス問題を受け、親会社のZホールディングスが立ち上げた「グローバルなデータガバナンスに関する特別委員会」最終報告は、「LINE社においてガバメントアクセスへのリスク等の経済安全保障への配慮ができていなかった」と指摘し、データ保管やガバナンスの改善を提言している。

ここで重要なこととしては、「LINE China 社から外部の組織に対して、LMP に関する情報の漏えいは認められなかった。」（２４頁）とされていることである。決して現に情報漏洩等が起こったことが問題とされているのではない。

しかし、大きく分けて経済安全保障とデータガバナンスに関する２つの重要なポイントが指摘されている。

第４　経済安全保障とデータガバナンス
２ 経済安全保障とデータガバナンスーLine事件を踏まえて

(3)Line事件に見る経済安全保障とデータガバナンス

１点目は、**経済安全保障への配慮**の必要性である。中国においてLineアプリのデータの一部確認を開始するにあたり、国家情報法等のように、個人情報保護法制そのものではないものの情報管理に影響を与え得る外国法制について、網羅的にはリサーチ対象に含めていなかった（20頁）。そのことにつき、報告書は、LINE社においては、通信の秘密を含むユーザーの個人情報を扱う以上、国家情報法に限らず広く中国におけるガバメントアクセスのリスクを慎重に検討する必要があったところ、ガバメントアクセスのリスクとしても受け止めて、経営上の課題として適切に取り上げ、ガバメントアクセスのリスクへの必要な対応を取ることができなかったと評している（25-26頁）。その結果として、ガバメントアクセスのリスクを含む経済安全保障分野に関する管理体制や事後的にもこれを見直す体制の整備が不十分であったことから、経済安全保障 を考慮したデータガバナンス体制を構築していく必要があるとされている（74－80頁）。

第４　経済安全保障とデータガバナンス
２ 経済安全保障とデータガバナンスーLine事件を踏まえて

(3)Line事件に見る経済安全保障とデータガバナンス

２点目は**コミュニケーションないしステークホルダーへの説明責任**である。すなわち、一部データが韓国のデータセンターに保存されていたにもかかわらず、対外的に「LINEの個人情報を扱う主要なサーバーは日本国内にある」「日本に閉じている」等の誤った説明をしていたということである（４４－５２頁）。

LINE 社が変わるべきことは、客観的な事実を誠実に伝えるという点にコミットすることである、報告書は、「ユーザーを裏切らない」ことを重視し、中長期的な視野に立って誠実なコミュニケーションを行うことを旨としなければならない。そしてそのことを、LINE社の役職員ひとりひとりが思いを致さなければならない等と強く批判している(８２頁)。

第４　経済安全保障とデータガバナンス
２ 経済安全保障とデータガバナンスーLine事件を踏まえて

(3)Line事件に見る経済安全保障とデータガバナンス

これは、あくまでもグローバルデータガバナンスの一部の問題が表面化しただけであり、この２点だけがデータガバナンスではない。しかし、この事件の反省を踏まえ、

①なぜ日本ではないその国にデータを置くのか、地政学リスク・地経学リスクをどのように考えてどうリスクを検討したのか、という点をステークホルダーに正確に説明できなければならない、その際には、いわば「まずいことに蓋をして」隠すのではなくむしろしっかりと説明（説明責任）しなければならない。

また、②経営者が、経済安全保障・ガバメントアクセスを含むデータガバナンスを経営上の重要な問題と捉え、トップとして責任感を持って対応していかなければならない。

第４　経済安全保障とデータガバナンス

３ 経済安全保障と日本企業（特に経営レベル）の対応

上記のとおりプライバシーガバナンスガイドブックは経営者が取り組むべき三要件として、①ガバナンスに係る姿勢の明文化、②保護責任者の指名及び③取組に対するリソースの投入を挙げていた。

このような経営者の取り組みの必要性を踏まえ、特に経営レベルでは、日本企業は経済安全保障に対して以下の対応をすべきである。

第４　経済安全保障とデータガバナンス

３ 経済安全保障と日本企業（特に経営レベル）の対応

①経済安全保障を考慮した意思決定機関・体制の整備

近時、経済安全保障の対応措置として、一部の企業は専門部署を設置するという動きが見られる。例えば、社長直轄の「経済安全保障統括室」を設置した企業がある。企業は経済安全保障を考慮するための必要な組織、体制を設置・見直し、意思決定機関の決裁・報告プロセスにおいて経済安全保障が考慮されるよう設計する必要がある。

第４　経済安全保障とデータガバナンス

３ 経済安全保障と日本企業（特に経営レベル）の対応

② 経済安全保障の観点に基づく事業リスクの評価

第二に、新規および既存の事業においても経済安全保障上のリスクがないかを検討し、またその後も定期的に点検・評価できる態勢を確保するべきである。

上記Line事件においては、事後的に見直す体制の整備が不十分と指摘されているので、この点は一度新規参入等の場面で検討した場合でも、その後も定期的に見直すことが重要である。

第４　経済安全保障とデータガバナンス

３ 経済安全保障と日本企業（特に経営レベル）の対応

③経済安全保障に関する情報収集・分析態勢の構築

第三に、企業の意思決定を支える経済安全保障関連の情報収集・分析の態勢・プロセスを整備することである。（経済）安全保障問題は複雑で流動的な面があり、企業・組織内部で完結することが難しく、外部の専門家・研究者の知見が必要となるだろう。１ 人の専門家がこの問題を全てカバーすることは極めて困難であるため、企業・組織としては自社に必要な個別具体的な問題領域やテーマ毎の専門家を把握しておくことが現実的である。外部の知見も含めて、必要な経済安全保障関連情報を収集・分析する態勢を構築する必要がある。

第４　経済安全保障とデータガバナンス

３ 経済安全保障と日本企業（特に経営レベル）の対応

④ 対外的コミュニケーション

第四に、企業は投資家やその他ステークホルダーとの間で経済安全保障に関する建設的対話を促すため、有価証券報告書を始めとする開示文書や自社ウェブサイト等において、経済安全保障に関するリスク認識・対応、各種機関・ 会議体における経済安全保障の議論の状況等に関する開示等のコミュニケーションを実施することが重要である。

このようなコミュニケーションの際はLine事件でも指摘されているように、「短期的」安心を与えるため海外での保管の事実や経済安全保障リスクを隠すのではなく、もし合理的な理由に基づき海外で保管するのであれば、そのような合理的理由を説明することで「長期的」な安心を与えるべきである。

第５　クラウド

１　外国にクラウドサーバが存在する場合の日本法の規制

クラウドサーバの利用については、2022年4月1日施行の「個人情報の保護に関する法律についてのガイドライン」に関するQ&A（以下「Q&A」という。）7-53が、「クラウドサービス提供事業者が、当該個人データを取り扱わないこととなっている場合には、当該個人情報取扱事業者は個人データを提供したことにはならない」とし、外国第三者提供についても「当該サーバを運営する外国にある事業者が、当該サーバに保存された個人データを取り扱わないこととなっている場合には、外国にある第三者への提供(略)に該当しません」（Q&A12-4）とされており、その場合には「自ら果たすべき安全管理措置の一環として、適切な安全管理措置を講じる 必要がある」（Q&A7-54）としていることが重要となる。以下では、「個人データを取り扱わないこととなっている場合」であることを前提に、第三者提供（改正法２７条）、外国第三者提供（改正法２８条）が適用されない前提での対応について簡単に説明する。

第５　クラウド

１　外国にクラウドサーバが存在する場合の日本法の規制

かかる場合においては、安全管理措置の一環としての外的環境の把握（個人情報の保護に関する法律についてのガイドライン（通則編）令和3年10月29日　（未施行:令和4年4月1日施行）［令和3年11月17日更新］１０－７）、すなわち、「個人情報取扱事業者が、外国において個人データを取り扱う場合、当該外国の個人情報の保護に関する制度等を把握した上で、個人データ の安全管理のために必要かつ適切な措置を講じなければならない。」という点に対応することが必要である。

このような場合、Q&A10-25は「外国において個人データを取り扱うこととなるため、当該外国の個人情報の保護に関する制度等を把握した上で、安全管理措置を講じる必要があります。日本国内に所在するサーバに個人データが保存される場合においても同様です。」とされている。

個人情報保護委員会は中国を含む３１の国や地域について、「年内を目途に、調査対象とする国又は地域の個人情報の保護に関する制度と我が国の個人情報保護法との間の本質的な差異の把握に資する一定の情報を公表する予定」としている。但し、この内容は「必要かつ適切な措置」の具体的内容を含まないと想定され、その意味では、中国の制度について個人情報保護委員会の公表を参照しながらも、自社の（経済安全保障リスクを含む）リスクの特徴を踏まえた独自の「必要かつ適切な措置」検討が必要であろう。

第５　クラウド

１　外国にクラウドサーバが存在する場合の日本法の規制

更に、このような外的環境の把握が安全管理措置の一環として行われる以上、「保有個人データの安全管理のために講じた措置」（改正法３２条１項４号、改正政令１０条１号）を本人の知り得る状態に置く義務にも対応する必要がある。

Q&A10-25が「クラウドサービス提供事業者が所在する外国の名称及び個人データが保存されるサーバが所在する外国の名称を明らかにし、当該外国の制度等を把握した上で講じた措置の内容を本人の知り得る状態に置く必要があります。」としていることが参考になる。

第５　クラウド

２　中国にクラウドサーバが存在する場合の中国法の適用関係−中国の公民の個人情報と日本居住者の個人情報を中国のクラウドサーバにアップロードすることを例にとって

（1）中国国内での保存義務

中国サイバーセキュリティー法第37条は、「重要情報インフラストラクチャーの運営者が中華人民共和国の国内での運営において収集、発生させた個人情報及び重要データは、国内で保存しなければならない。業務の必要性により、国外に対し確かに提供する必要のある場合には、国のネットワーク安全情報化機関が国務院の関係機関と共同して制定する弁法に従い安全評価を行わなければならない。法律及び行政法規に別段の定めのある場合には、当該定めに基づいて行う。」と規定している。また、中国個人情報保護法40条は「重要情報インフラストラクチャー運営者及び取扱う個人情報が国家インターネット情報部門の規定する数量に達した個人情報取扱者は、中華人民共和国域内で収集し又は発生した個人情報を域内で保存しなければならない。確かに域外に提供する必要がある場合には、国家インターネット情報部門による安全評価　に合格しなければならない。法律、行政法規及び国家インターネット情報部門が安全評価を行わなくて良いと規定する場合には、その規定に従う。」とする。つまり、サイバーセキュリティー法が重要インフラストラクチャー運営者のみに国内保存義務を課し、個人情報保護法はこれに加え、「取扱う個人情報が国家インターネット情報部門の規定する数量に達した個人情報取扱者」にも国内保存義務を課している。

第５　クラウド

２　中国にクラウドサーバが存在する場合の中国法の適用関係−中国の公民の個人情報と日本居住者の個人情報を中国のクラウドサーバにアップロードすることを例にとって

(1) 中国国内での保存義務（データローカリゼーション規制）

重要インフラストラクチャー運営者は、2021年8月17日に公布された重要情報インフラ安全保護条例によれば、重要情報インフラストラクチャーとは、公共通信及び情報サービス、エネルギー、交通、水利、金融、公共サービス、電子政務、国防科学技術工業等の重要な業界及び分野、及び破壊、機能喪失又はデータ漏洩を受ければ、国家の安全、国家経済、民生、公共の利益に深刻な危害を及ぼす可能性のあるその他の重要なネットワーク施設、情報システム等を指す。

重要情報インフラの認定基準については、同条例、上記の重要な業界及び分野の主管部門、監督管理部門が責任を持って重要な情報インフラ認定規則を制定し、当該業界、当該分野の重要情報インフラを認定すると規定している。

電信業務について、工業・情報化部門は、まだ重要情報インフラを認定していないものの、2016年に効力が発生した「国家サイバーセキュリティ検査操作ガイドライン」によれば、電信とインターネット業界について、クラウドサービスは、重要情報インフラと指定されている。したがって、今後も、クラウドサービスが重要情報インフラとして指定される可能性が高いと考えられる。したがって、中国のクラウドベンダーは、中国サイバーセキュリティー法第37条に基づき、原則として中国で保存しなければならない。

第５　クラウド

２　中国にクラウドサーバが存在する場合の中国法の適用関係−中国の公民の個人情報と日本居住者の個人情報を中国のクラウドサーバにアップロードすることを例にとって

(1) 中国国内での保存義務（データローカリゼーション規制）

また、今後の規定状況にもよるが、中国のクラウドベンダーが「取扱う個人情報が国家インターネット情報部門の規定する数量に達した個人情報取扱者」に該当する可能性も十分にある。

なお、日本居住者の個人情報を中国のクラウドサーバにアップロードする場合でも、例えば、中国におけるECサイトにアクセスした日本居住者の個人情報等であれば、ネットワーク運営者にとっては、これは、中国国内での運営において収集した個人情報と判断される可能性があることから、その意味で保守的に考えると、日本居住者の個人情報なら中国のサーバにアップロードしても国内保存義務と無関係とは断言できないことになるだろう。

第５　クラウド

２　中国にクラウドサーバが存在する場合の中国法の適用関係−中国の公民の個人情報と日本居住者の個人情報を中国のクラウドサーバにアップロードすることを例にとって

(2) データの国外移転

上記の通り、情報安全技術データ国外移転安全評価ガイドラインがデータの国外移転について規定していたところ、「ガイドライン」は、さらに次に掲げる状況のいずれかもデータの国外移転に該当するとした。①本国国内にあるものの、本国司法管轄に属しない又は国内で登録されない主体に対して個人情報と重要データを提供する場合。②データは、本国以外のところに移転されないが、国外の機構、組織、個人がアクセスし閲覧される場合（公開された情報、ウェブサイトのアクセスを除く）。③ネットワーク運営者グループ内部のデータが国内から国外に移転され、国内の運営に収集し発生させた個人データと重要データに関わった場合。つまり、クラウドサービスにおけるデータは、中国国外の企業（例えば日本企業）がこれをアクセスすることができる（いわゆるリモートアクセス）場合であっても、データの国外移転と見なされる可能性がある。

そして、全ての個人情報取扱者に課される一般的な域外移転のルールは上記第３の１のとおりであるが、国内保存義務が課せられた場合に例外的に域外提供が認められるのは、「確かに域外に提供する必要がある場合」であり、かつ国家の安全評価を受けた場合に限られる。

第５　クラウド

２　中国にクラウドサーバが存在する場合の中国法の適用関係−中国の公民の個人情報と日本居住者の個人情報を中国のクラウドサーバにアップロードすることを例にとって

(3)データインターフェースの提供

上記第２の５のとおり、2016年1月1日から施行された反テロリズム法第18条は、電気通信業務経営者、インターネットサービスプロバイダは公安機関、国家安全機関によるテロ活動の調査に技術インターフェースや機密解除などの技術サポートを提供しなければならないと明確に規定している。

また、国家強制基準である『情報セキュリティ技術インターネットインターラクティブサービスのセキュリティ保護要求』第13.4条では、インターネットインターラクティブサービスの提供者が公安機関にコンプライアンスに準拠した技術インターフェースを提供し、リアルタイムかつ効果的に関連証拠を提供することを確保しなければならないことを要求している。

第５　クラウド

２　中国にクラウドサーバが存在する場合の中国法の適用関係−中国の公民の個人情報と日本居住者の個人情報を中国のクラウドサーバにアップロードすることを例にとって

(3)データインターフェースの提供

クラウドに関する具体的な状況として、反テロリズム法第18条に基づく技術インターフェースや機密解除などの技術サポートを提供の可能性は否定できない。

但し、関係国家機関が法的手続きを経ずにビジネスデータを勝手に取得することができるということになるわけではない。

第６　その他の中国の最新動向

１　取り締まりの強化

個人情報保護法の施行に伴い、中国政府は、個人情報の取り扱いに問題がある企業に対する取締りを強化している。

2021年11月1日に、工業と情報化部は、「情報通信サービスの感度向上行動の展開に関する通知」を発表した。当該通知によると、各関連企業は2021年12月末までに「収集済み個人情報リスト」と「第三者と共有した個人情報リスト」を作成し、アプリのメニュー上に表示し、ユーザーの問い合わせに供しなければならない。収集済み個人情報リストは、アプリが収集したユーザーの個人情報の基本的な状況（情報の種類、使用目的、使用シナリオなど）を簡潔かつ明確に記載しなければならない。第三者との個人情報共有リストには、第三者と共有する個人情報の種類、使用目的、使用シナリオ及び共有方法等の内容が含まれる。アプリが第三者と共有するユーザーの個人情報の基本状況を簡潔かつ明確に記載しなければならない。

工業情報化部は2021年11月16日、「第14次五カ年計画情報通信業界発展計画」の記者会見を開いた。工業情報化部情報通信管理局の王鵬副局長は、「これまでに21回で計244万アプリの検査を実施し、累計2049件の違反アプリを通報した。修正を拒否した540件のアプリを撤去させ、違反行為に対する高圧的な抑止力を維持し続けている」と述べた。

第６　その他の中国の最新動向
１　取り締まりの強化

11月24日、中国中央テレビニュースの報道によると、今年に入って工業情報化部が展開したアプリによるユーザー権益侵害特別取り締まりキャンペーンでは、テンセントの9製品に違反行為があったとされた。工業情報化部はテンセント社に対して経過的な行政指導措置をとり、今後発表されるアプリの新製品、および既存のアプリの更新版について、工業情報化部が技術検査を実施し、検査に合格した後に投入することを要求した。

https://maimai.cn/article/detail?fid=1685404195&efid=4SBOptawsiT7QHAzogFaFQ

第６　その他の中国の最新動向
２　「データ税」？

2021年10月、前重慶市長である黄奇帆氏は上海外灘金融サミットでデータ税を提唱し、企業がユーザーデータを収集することで得た収益を統計し、その20～30%をデータ税として回収するよう提案した。これは中国共産党政府が新たな税金を投入する際の「観測気球」ではないかとされている。このようなデータ税の概念は、中国政府が打ち出す「共同富裕」と軌を一にする。そこで、タオバオを保有するアリババやウィーチャットを保有するテンセントが課税対象としてされて、税率は3割程度になると予想されている。

https://www.sohu.com/a/440161314_614005

Thanks.

メールでのご質問先は以下の通りです。
tmatsuo@llm13.law.harvard.edu

本発表準備においては桃尾・松尾・難波法律事務所胡悦律師に多大な協力をいただいた。ここに再度感謝の意を表する。