SQUIRE PATTON BOGGS

China's Draft Data Security Measures and How They Compare to the GDPR
中国的数据安全办法草案及其与欧盟《通用数据保护条例》的比较

The Cyberspace Administration of China (CAC) launched a public consultation on the draft Administrative Measures on Data Security (Draft Measures) on May 28, 2019. This consultation falls in the middle of the publication of the drafts for two other data protection rules, namely the Measures for Security Assessment for Cross-border Transfer of Personal Information and the Measures for Cybersecurity Review.

中国国家互联网信息办公室（以下简称“网信办”）于2019年5月28日就《数据安全管理办法（征求意见稿）》（以下简称“《办法》”）向社会公开征求意见。而这次征求意见的时间正值另两项数据保护规则公布之际，即《个人信息出境安全评估办法》和《网络安全审查办法》。

Together, these three measures will implement a significant portion of the Cyber Security Law (CSL) and become the first set of binding laws focused solely on data protection, adopting certain rules from the non-binding Personal Information Security Specification. The Draft Measures were published just over a year after the General Data Protection Regulation (GDPR) came into effect in the EU and certain similarities between the two regimes are apparent.

这三项《办法》结合起来，将共同落实《网络安全法》的重要部分，成为首批致力于数据保护的一整套具有约束力的法律，并采纳了非强制性的《个人信息安全规范》中的一些规则。《通用数据保护条例》在欧盟生效后一年多时间内，本《办法》即获出台，两项制度之间的一些相似之处很明显。

Extraterritorial Scope
域外效力

The territorial scope of the CSL is repeated in Article 2 of the Draft Measures, to the extent that it shall apply to the construction, operation, maintenance and use of the network, as well as the supervision and administration of cybersecurity within the country. However, Article 4 of the Draft Measures further stipulates that the State will "monitor, defend against and deal with data security risks and threats from both inside and outside the territory of the People's Republic of China, protect data from being divulged, stolen, falsified, damaged or used illegally, and punish the illegal and criminal activities that endanger data security in accordance with the law".

《办法》第2条重申了《网络安全法》适用的地域范围，其适用于国内网络的建设、运营、维护和使用以及网络安全的监督和管理。但是，《办法》第4条进一步规定，国家将“监测、防御、处置来源于中华人民共和国境内外的数据安全风险和威胁，保护数据免受泄露、窃取、篡改、毁损、非法使用等，依法惩治危害数据安全的违法犯罪活动。”

It seems that China could take action against risks even outside of its borders, an extension of scope made even more powerful through the lack of a definition for the key terms "risks and threats".

由此看来，中国似乎拟对境外的风险采取措施。在缺少对“风险和威胁”这一核心术语作出定义的情况下，法律的适用范围还可以被进一步扩大。

As the CSL takes precedence over the Draft Measures, the latter are not allowed to make any provisions inconsistent therewith or create new law going beyond the implementation of rules in the CSL. Additionally, State overreach into other jurisdiction in order to protect from security threats is a regular phenomenon that can be committed by any government around the world. Consequently, different from the GDPR, the Draft Measures may not be interpreted as providing extraterritorial effect for data protection. Further clarity on what actions the State may take has not yet been provided. While the GDPR was criticized by commentators for expanding jurisdiction to protect any EU citizen, the Draft Measures might go even further on the basis of dealing with data security risks from outside China.

由于《网络安全法》的效力高于《办法》，后者不得作出任何与之不一致的规定，或创造超出《网络安全法》现行规则的新法律。此外，为了保护本国及其公民免受安全威胁，国家为防御国家安全风险而延伸管辖权是世界上任何政府都会实施的常见现象。因此，不同于《通用数据保护条例》，本《办法》不能被解释为赋予了数据保护域外效力。国家会采取何种措施尚需进一步澄清。尽管《通用数据保护条例》在扩大管辖权以保护所有欧盟公民的问题上遭到了评论人士的批评，但本《办法》可能会在处理来自中国境外的数据安全风险问题上更进一步。

Filing System/Registration Requirement
备案系统/注册要求

While, similarly to Art. 2(1), 4(6) and Recital 15 of the GDPR, the Draft Measures refer to "filing" requirements, the new procedure described in Article 15 is much more similar to the registration requirements under the implementation laws of the Data Protection Directive (the predecessor of the GDPR). How the filing system will work in practice is currently unclear and the government is seeking public opinion.

与《通用数据保护条例》第2条第1款，第4条第6款以及序言第15条类似，《办法》也提到了备案的要求，《办法》第15条所述的新程序与《数据保护指令》（即《通用数据保护条例》的前身）实施时规定的注册要求更为相似。备案系统实际上将如何运行目前尚不清楚，政府正在征求公众意见。

Perhaps the CAC may go in the direction the CNIL (France's data protection authority) took. Under French law, controllers had to register with the authority not only their own details, but also information on all processing and data transfers they or a processor undertakes. This also encompassed a requirement for controllers to register all new transfers and purposes of processing with the CNIL and await their consent.

也许网信办可能会效仿CNIL（法国数据保护机构）的做法。根据法国法律，数据管控者不仅要向当局登记他们自己的详细信息，还要登记所有有关他们或其他数据处理者处理转移数据的信息。这还包括要求管控者向CNIL登记所有新的转移情况和处理目的并等待他们的同意。

On the other end of the spectrum, the CAC may follow the ICO's example (the UK's data protection authority). The ICO had a template on its website with checkboxes, which would automatically generate statements when clicked. Thus, in contrast to drafting a complex registration document from scratch, as required in France, in the UK controllers simply had to decide which pre-existing statements applied to them. Also in contrast with the CNIL, the ICO did not need to provide consent for companies to process data, they only had to be informed. Considering the UK approach's advantage in efficiency and the CAC's fraternizing with potential offenders (which the ICO also formerly engaged in), the State will most likely consider the UK's implementation of the notification requirement.

另一方面，网信办可能会遵循ICO（英国的数据保护机构）的例子。ICO在其网站上有一个带有复选框的模板，这些复选框会在点击时自动生成陈述。因此，与法国要求的从头开始起草一份复杂的登记文件相比，英国的数据管控者只需决定哪些现成的陈述适用于他们。同样，与CNIL相比，公司处理数据不需要经过ICO 的同意，只需要通知他们。鉴于英国的做法在效率方面的优势以及网信办与潜在违法者保持友好关系的需要（ICO之前也这样做），国家很可能会考虑采用英国所实施的通知要求。

It is worth noting that, in line with Recital 89 GDPR, the requirement to register with local authorities in the EU was overturned in the GDPR. This served to replace the external accountability requirement of notification with internal accountability measures, such as maintaining accurate Records of Processing and conducting Data Protection Impact Assessments, which the authorities can access. Nevertheless, it can be argued that the ICO's current requirement to pay a data protection fee is a sort of work-around of the prohibition on a blanket registration requirement. Additionally, the CNIL (like the AEPD in Spain and the ADA in Lithuania) still has a form of Controller registration requirement and the Estonian data protection authority still requires the processing of sensitive data to be registered, perhaps reflecting the Article 15 requirement the most.

值得注意的是，根据《通用数据保护条例》序言第89条，在欧盟地方当局注册的要求已被条例的规定所推翻。这有助于用内部问责措施取代通知要求这种外部问责，例如保持处理记录的准确，开展数据保护影响评估，且可供当局获得。然而，ICO目前支付数据保护费的要求被认为是对禁止全面注册要求的一种变通做法。

此外，CNIL（如同西班牙的AEPD以及立陶宛的ADA）仍然有管控者注册要求的形式，爱沙尼亚的数据保护机构仍然要求对敏感数据的处理进行注册，这些可能最能对应《办法》第15条的要求。

Big Data and VPN

大数据和VPN

Perhaps the biggest areas of divergence between the GDPR and the Draft Measures are their treatment of big data and the use of VPN. The GDPR covers big data and AI indirectly in Article 22, in its rights related to automated decision making. Through the right to object conferred therein, together with elements like data security requirements, the EU clearly opted to restrict big data in favour of consumer protection.

也许《通用数据保护条例》和《办法》最大的分歧是它们对于大数据的处理和VPN的使用。《通用数据保护条例》在第22条，与自动化决策相关的权利中间接地涵盖了大数据和人工智能。通过在条款中赋予反对权以及数据安全要求等要素，欧盟明确地选择限制大数据以利于消费者保护。

By contrast, through the Draft Measures, China seems to limit mass data collection only to where required for the sake of transparency. Article 16 of the Draft Measures explicitly requires network operators to abstain from interfering with automatic data collection and access, mandating that they only stop doing so when they "seriously affect the operation of websites". Article 24 adds a transparency requirement, that network operators automatically synthesizing media information indicate explicitly this process. The only restriction on big data and AI is contained in Sentence 2 of Article 24, which prohibits the aforementioned use in media information synthesis for the aims of causing profit increase or damage.

相比之下，《办法》似乎只在要求透明度的层面对大规模数据的收集予以限制。《办法》的第16条明确要求网络运营者不得干扰自动数据收集和访问，要求自动化访问收集仅当在“严重影响网站运行”时方可停止。第24条增加了一项透明度要求，即网络运营者必须清晰地标识出自动合成媒体信息的过程。对大数据和人工智能的唯一限制载于24条第2句，禁止以谋取利益或损害他人利益为目的使用前述的媒体信息合成技术。

Thus, the Draft Measures seem to align more with the California Consumer Protection Act (CCPA) than the GDPR, which simply does not mention automated decision making. The reasons thereof can perhaps be found in the high technological aims of their countries. Through lax regulation of big data, the CCPA may aim at supporting innovation in Silicon Valley and the Draft Measures at doing the same in Shenzhen.

因此，《办法》似乎相较于《通用数据保护条例》更接近《加州消费者保护法》（“CCPA”），其中根本未提到自动化决策。其原因或许在于国家的高技术目标。由于对大数据的宽松监管，CCPA能够致力于支持硅谷的创新，而《办法》也将在深圳起到同样的效果。

However, the commercial advantage provided by Articles 16 and 24 may be undone by the strengthening of the Great Firewall in Article 29. This article generally prohibits the overseas routing of traffic on domestic internet by domestic users, which seems to be a direct attack on the use of VPN. Nevertheless, the article in the Draft Measures is too brief to guide practitioners in this regard. Future regulation or guidelines may provide interpretations of the definition and limitations of the overseas routing of traffic.

然而，《办法》第16条和24条带来的商业优势可能会因第29条的限制而削弱。该条款一般禁止国内用户在国内互联网上将流量路由到境外，这似乎是对使用VPN的直接限制。然而，《办法》中的条款过于简短，难以指导实践中该方面的工作。将来的法规或指南可能会解释流量境外路由的定义和限制。

Marketing Rules

市场营销规则

Another similarity to the GDPR is likely to be the new marketing rules provided by Article 23 of the Draft Measures. Article 21 GDPR provides data subjects the right to object to direct marketing and adds some transparency requirements to be implemented by controllers and processors. Similarly, Article 23 of the Draft Measures requires network operators to explicitly indicate where data is used for targeted advertisement and gives users the right to object to receiving such advertisements. The Article also sets out the procedure to be followed, requiring operators to stop push advertising when the user opts out and to delete their data.

另一个与《通用数据保护条例》的相似之处可能是《办法》第23条中规定的新营销规则。《通用数据保护条例》第21条规定了数据主体反对直接营销的权利，以及对控制者和处理者施加了透明度的要求。同样，《办法》第23条要求网络运营者明确指出目标广告的数据使用地点，并且赋予用户拒绝接受此类广告的权利。该条款也列出了需遵循的程序，要求运营者在用户选择退订时停止推送广告并删除其数据。

The conditions for consent to marketing (and other processing) are also brought in line with the EU. In Article 7, the GDPR sets out the elements of free, informed and clear consent. Similarly, Article 11 of the Draft Measures prohibits consent by default, bundling and implied consent.

同意营销（以及其他处理）的条件也与欧盟一致。在第7条中，《通用数据保护条例》列明了在知情的前提下作出自主、和明示的同意的要求。同样，《办法》第11条禁止 默认授权、捆绑以及默示同意。

Nevertheless, Article 23 of the Draft Measures still provides some additional powers to the enforcement agencies that the GDPR does not. Specifically, Paragraph 2 requires network operators engaged in targeted advertising to "respect social morality and business ethic, abide by public order and good morals, and be honest and diligent". The vague wording thereof may empower enforcement agencies to clamp down on businesses in a wide-ranging array of situations unless further guidance is provided.

尽管如此，《办法》第23条依旧向执行机关赋予了《通用数据保护条例》中并未赋予的额外权力。具体而言，其第2款要求开展定向广告推送的网络运营者"尊重社会公德、商业道德、公序良俗，诚实守信"。这些措辞可能使执法机构在比较大的范围内有自由裁量权，除非出台进一步的指引。

Penalties

处罚

Ultimately, the potential for severe penalties in the cases of non-compliance is the biggest motivator of compliance. Compliance with the GDPR was undoubtedly so high due to the high value of potential fines. The Draft Measures followed this line in Article 37, increasing the seriousness of potential remedies, but nevertheless failing to reach the levels of the GDPR. Similarly to previous provisions, the Article sets out examples of the disciplinary action that enforcers can take, ranging from "disclosing misconduct publicly, confiscating illegal incomes, [and] suspending relevant business operations" to "ceasing business operation for rectification, shutting down the websites, [and] revoking the relevant business permits or business licenses on it".

归根结底，合规的最大推动力在于不合规时可能受到的严厉处罚。《通用数据保护条例》下的合规程度因为潜在的高额罚款，无疑相当之高。《办法》在第37条中遵循沿袭了这一原则，增加了潜在措施的严厉性，但仍未达到《通用数据保护条例》的级别。与之前的规定相似，该条款列举了执法者可以采取的惩戒措施，从"公开曝光、没收违法所得、暂停相关业务"到"停业整顿、关闭网站、吊销相关业务许可证或吊销营业执照"。

Notably, the Draft Measures did not list the imposition of monetary penalties as one of the available enforcement tools and they did not set out the extent thereof in a separate article, like Article 83 of the GDPR. The reasons thereof remain unclear and will perhaps be explained in future guidance.

值得注意的是，《办法》并未将罚金列为可实施的执法手段之一，也没有像《通用数据保护条例》第83条一样，在单独的条款中列出处罚的力度。其原因尚未明确，可能会在未来的指导方针指引中加以解释。

The Draft Measures are currently up for consultation. Any member of the public can provide comments until June 28, 2019.

《办法》目前正在公开征求意见。公众可在2019年6月28日前发表评论。

About Us

关于本所

More than 1,500 lawyers in 47 offices across 20 countries on five continents provide unrivalled access to expertise.

分布在五大洲20个国家47间分所的1,500多名律师为客户提供竞争者难以企及的专业服务。

The combination of our comprehensive knowledge of political climates and regulatory landscapes, together with our grasp of the intersection of business, law and government, has led to our reputation for cutting-edge advocacy work. We are consistently recognized by publications.

我们兼具政治气候和监管环境的综合知识，加之对商务、法律和政府事务的全面把握，使我们在前沿的公共政策倡导领域闻名遐迩，并一直获得媒体的赞誉。

Contacts

联系我们

Kelly Liu 刘佳
合伙人，北京
Partner, Beijing
T +86 10 6589 3782
E kelly.liu@squirepb.com

Daniel Csigirinszkij
律师助理，伦敦
Paralegal, London
T +44 20 7655 1489
E daniel.csigirinszkij@squirepb.com