2016 年 8 月

众达法律评论

欧盟网络安全新指令：对数字服务提供者有什么影响？

继 2016 年 7 月 6 日欧洲议会通过《网络与信息安全指令》（“NIS 指令”），并于 2016 年 7 月 19 日在欧盟官方公报公布之后，2016 年 8 月 8 日，NIS 指令正式生效。负责数字单一市场的欧洲委员会副主席 Andus Ansip 称，“该指令是欧盟关于网络安全首部全面的立法，是我们发展该领域的构建基石”。的确，NIS 指令将通过对欧盟成员国实施最低限度的协调性规则，以提供相应措施来促进欧盟的整体网络安全水平。

NIS 指令对两类实体提供了相应指南：(i) 能源、交通、银行业、金融市场基础设施、医疗、饮用水和数字基础设施领域的“基础服务运营者”，和 (ii) 包括比如网上市场、在线搜索引擎和云计算服务提供者等实体在内的“数字服务提供者”。

NIS 指令草案涵盖数字服务提供者一事引起了大量争论，受到了来自欧洲议会、多个成员国以及被归入“数字服务提供者”定义下的实体的反对。这些反对者认为针对数字服务提供者的网络攻击不足以构成重大事件，因此反对额外的规定，因为额外规定可能对创新产生消极影响。虽然 NIS 指令终稿包含了数字服务提供者，但与基础服务运营者相比，NIS 指令对其采取了较为宽松的管制。[1]

就本《评论》而言，我们将主要聚焦这类数字服务提供者。

相关条款

“数字服务提供者”（“DSP”）是指“通常经接收服务的个人请求，以电子方式[2]远距离提供有偿服务”的法人。

值得注意的是，依照 NIS 指令的前言规定所述，数字服务提供者并不包括“硬件生产者和软件开发者”。因此，对数字服务提供者虽要求其技术性和组织性措施保持“最先进水平”，但“并不要求以特定方式设计、开发或

生产特定商业信息和通信技术产品”。于是，NIS 指令虽然包含前言规定强调软硬件开发者使基础服务运营者和数字服务提供者得以保护其网络与信息系统安全的关键角色，指令并未对此作出额外规定。诚然，软硬件产品已受限于与产品责任相关的现行规定。

数字服务提供者的服务涵盖以下三类服务（NIS 指令（附件 III））：“在线市场”、“在线搜索引擎”和“云计算服务”：

- **“在线市场”**包括“允许消费者和/或交易者在在线市场的网站或采用在线市场提供计算服务的交易者网站，与交易者达成在线销售或服务契约的一类电子服务”。正如 NIS 指令的前言规定所示，该定义未涵盖仅作为第三方服务的中间媒介来达成最终契约的在线服务。
- **“在线搜索引擎”**包括“允许使用者基于关键词、短语或其他输入形式的任何内容的搜索请求，搜索所有网站或某一特定语言的网站，而出现的链接中包含与搜索的内容相关的信息的一类电子服务”。NIS 指令的范围既不包括对仅限于特定网站内容搜索的功能的提供，也不包括就各类交易者的特定产品或服务的价格进行比较的服务。
- **“云计算服务”**指“能提供获取可扩展的、弹性的可共享计算资源库渠道的一类电子服务”。根据 NIS 指令的前言规定，这种计算服务包括比如网络、服务器或其他基础设施、存储、应用和服务在内的资源。

值得注意的是，在立法阶段，就其他服务类别的供应者的规定产生了争议，比如流媒体、主要在线网络游戏、应用软件的数字发布平台和社交网络提供者，但它们最终被排除在指令范围之外。

数字服务提供者的义务

安全要求。NIS 指令旨在实施“最先进水平”的措施。它需要数字服务提供者：

- 明确在欧盟境内提供服务时采用的网络与信息系统的安全性所面临的风险，并采取适当的技术性和组织性措施来管理此类风险。这些措施必须保持“最先进水平”并考虑以下因素：(i) 系统与设施的安全；(ii) 突发事件管理；(iii) 业务持续性管理；(iv) 监控、审计与测试；和(v) 遵守国际标准。
- 为确保服务的连续性，采取措施防止突发事件对在欧盟境内提供服务的网络与信息系统安全产生影响，并最小化该种影响。

突发事件通知要求。发生对欧盟境内提供服务有重大影响的任何突发事件，数字服务提供者必须立即告知主管机构或欧盟成员国指定的“计算机安全应急响应小组”（“应急响应小组”）。通知必须包括能使主管机构或应急响应小组确定任何跨境影响严重性的信息。但是，通知方不因该通知而负更多责任。

在确定突发事件影响的重要性时，应考虑 NIS 指令中的以下因素：

- 受突发事件影响的用户数量，特别是依赖该服务来提供自身服务的用户；
- 突发事件的持续时间；
- 受突发事件影响区域的地理分布；
- 服务功能的破坏程度；
- 对经济和社会活动的影响程度。

只有当数字服务提供者已获取需对突发事件就上述因素有关的影响进行评估的信息时，通知义务才适用。

指令的实施、通知后程序和强制执行

关于 NIS 指令的实施，欧盟成员国需要采取指令就欧盟境内网络安全监管措施的策略，创建欧盟成员国解决跨境安全突发事件的计算机安全应急响应团队，并成立鼓励欧盟成员国交换信息的统一战略合作小组。

网络与信息系统安全的国家策略。欧盟成员国必须采取具有明确目标的国家策略以及合适的政策和监管措施，以实现高级别的安全。为此，欧盟成员国必须指定：

- 负责协调问题促进跨境合作的国家单一联络点；
- 通过提供预先警告和警报、与利益相关者分享关于突发事件和风险的信息、建立关于在线活动和相关风险的公共意识、并致力于发展网络安全标准化实践，负责以国家层面来处理风险和突发事件的一个或多个应急响应小组。

通知后程序。在咨询过相关数字服务提供者后，如果被通知的主管机构或应急响应小组（及适用情况下其他相关的欧盟成员国机构或应急响应小组）认定为了阻止突发事件或对正在进行中的突发事件作出响应，有必要引起公众注意，或认定披露突发事件以其他形式关乎公众利益，则可向公众告知个别突发事件或要求数据服务提供者做此告知。

强制执行。若有证据表明数字服务提供者并未遵守安全通知或突发事件通知的规定，欧盟成员国应确保主管机构采取行动；如有必要，可通过事后监督活动进行。这些证据可由提供服务所在的其他成员国的主管机构提交。

关于上述事后监督，主管机构有权：

- 要求数据提供者提供评估他们的网络和信息系统安全性所需的信息，包括有明文规定的安全政策；
- 要求数据提供者对任何不符合安全和突发事件通知要求的事项进行救济。

NIS 指令要求欧盟成员国制定适用于违反依据指令而采用的国家规定的处罚规则，并采取所有必要措施确保这些规则的强制实施。处罚仅需是“有效、适当且有劝诫性的”，因此每个成员国可自行就不合规的行为制定具体的制裁规定。

指令的管辖权和领土权/治外法权的范围

数据服务提供者被视为受其主要设立地点（即总部）所在的欧盟成员国的司法管辖。

如果数据服务提供者的主要设立地点在某欧盟成员国境内，但其网络和信息系统却位于另一个或其他几个成员国，则该主要设立地点所在的成员国的主管机构和其他成员国主管机构必须进行相互合作和协助。

为促进安全规定和突发事件通知程序的统一实施，NIS 指令鼓励相关规则的标准化。

主要设立地点在欧盟境外的数据服务提供者若在欧盟境内提供服务，仍可能被纳入指令范围之内。若此，他们必须在欧盟境内指定一名代理人。不过，根据 NIS 指令，仅通过在欧盟境内可登陆数据服务提供者的网站，或可获取其电子邮箱地址或其他联系方式，并不足以构成此等判断。然而，因素诸如数据服务提供者使用在一个或多个欧盟成员国普遍使用的语言或货币，且可以此等语言定制服务，和/或提及位于欧盟的顾客或使用者，可使得该数据服务提供者实际上设想在欧盟境内提供服务的事实显而易见。

与一般数据保护规定的关系

作为数字服务提供者的数据控制器和处理器可能同时受制于 NIS 指令和《一般数据保护条例》（“GDPR”）（2016 年 4 月 27 日第 2016/679 号（欧盟）条例），后者涵盖了欧盟数据主体的各类新保护措施，以及对不合规行为的重大罚款和惩罚。因此数据保护突发事件可能同时触发两项规定下的通知义务。

但是，NIS 指令和 GDPR 下的数据保护类型有重大区别。NIS 指令涵盖了数据泄漏的任何类型，而 GDPR 下的保护数据则限于“个人数据”，其定义是“关于明确的或可确定的自然人（“数据主体”）的任何信息”。

此外，NIS 指令不仅包含数据泄漏，也包含能够影响数字服务提供者网络安全和影响服务提供的任何“突发事件”。

展望

欧盟成员国将在 2018 年 5 月 9 日之前，将 NIS 指令落实到期国家法律中。

NIS 指令将要求数字服务提供者和其他相关实体在符合指令规定的前提下，仔细审查现有网络安全并建立适当的突发事件通知措施。

NIS 指令范围内的实体必须实施“最先进水平的”安全措施，“应确保与风险相适应的安全级别”。为落实这一安全级别，企业必须要有可审计的综合安全计划。为做好准备工作，企业应：

- 在高级管理层内部指定个人或小组评估 NIS 指令对该企业的适用性，并发展准备计划 。
- 进行安全影响评估。

- 审查所有的内部安全程序，并做好国家机关规定的自我审计能力。
- 配合董事会、主要法务专员和其他高级管理人员，采取内部安全和应急响应策略。
- 遵守泄密报告的规定，迅速实施突发事件应急响应计划。
- 考虑采取将新的 NIS 威胁信息共享计划纳入在内的安全策略。

NIS 指令或将涉及欧盟境外设立的实体，这使得各公司需要评估其活动是否可能导致其被纳入指令范围。鉴于各个欧盟成员国还未确定对违规行为的处罚，各公司更需要确保自身未与 NIS 指令产生冲突。

联系律师

若想获取更多信息，请联系您的律所委托代表或以下所列律师之一。普通邮件信息可通过我们的“联系”表格进行发送，详见 www.jonesday.com/contactus/

袁黎明
上海
+86.21.2201.8106
lyuan@jonesday.com

Undine von Diemar
慕尼黑
+49.89.20.60.42.200
uvondiemar@jonesday.com

Jörg Hladjk
布鲁塞尔
+32.2.645.15.30
jhladjk@jonesday.com

Mauricio F. Paez
纽约
+1.212.326.7889
mfpaez@jonesday.com

Todd S. McClelland
亚特兰大
+1.404.581.8326
tmcclelland@jonesday.com

Gregory P. Silberman
硅谷
+1. 650.739.3954
gpsilberman@jonesday.com

Jonathon Little
伦敦
+44.20.7039.5224
jrlittle@jonesday.com

Rémy Fekete
巴黎
+33.1.56.59.39.90
rfekete@jonesday.com

Elizabeth Robertson
伦敦
+44.20.7039.5204
erobertson@jonesday.com

Rhys E. Thomas
伦敦
+44.20.7039.5101
rethomas@jonesday.com

Paloma Bru
马德里
+34.91.520.3985
pbru@jonesday.com

Laurent De Muyter
布鲁塞尔
+32.2.645.15.13
ldemuyter@jonesday.com

Olivier Haas
巴黎
+33.1.56.59.38.84
ohaas@jonesday.com

Giuseppe Mezzapesa
米兰
+39.02.7645.4001
gmezzapesa@jonesday.com

注释

[1] 例如：数字服务提供者只需就具有“实质影响”的突发事件进行通知，而基本服务运营者必须就任何具有“重大影响”的突发事件进行通知，而“重大影响”涉及的范围更为宽泛，且认定此类突发事件的指标的定义更狭窄。

[2] “电子手段”包括那些“为处理（包括数字压缩）和存储数据通过电子设备在其终端进行最初发送和接收，以及完全通过电报、无线、光纤手段或其他电磁手段传送、传达和接收”的服务（2015 年 9 月 9 日欧洲议会和欧洲理事会第 2015/1535 号（欧盟）指令第 1(1)(b)条，规定了技术条例和信息社会服务规则领域的信息规定程序）。

以上文章为翻译版，阅读英文原版请点击：http://www.jonesday.com/the-new-eu-cybersecurity-directive-what-impact-on-digital-service-providers-08-24-2016/