数据脱敏5 | 数据脱敏的法律效果是渐进的吗？

合规科技系列文章 **Law-Tech Series**

高速发展的时代背景下，一方面行业分工在层层细化，一方面跨学科的交叉研究又越来越不可或缺。科技与法律表面上是两个相去甚远的专业领域，但就数据治理与隐私保护而言，只有跨界互通才可能找到最佳的解决方案。

“合规科技专题文章”旨在兼顾科技与法律的双重视角，深度解读数据技术的逻辑原理与数据合规的法律要求，从而促进技术人与法律人的双向理解，探讨数据利用与个人权益协调发展的可行方案。

“大数据”已然从热词变成日常，而数据在释放无限潜力的同时，也引发了隐私泄露的巨大隐患。从若干年前科技公司野蛮生长，到近年来数据立法接踵而至，信息社会正在两极之间寻求平衡。数据脱敏提供了这样一种可能性——通过降低数据与主体之间的关联，可以同时保留较高的隐私保护程度和较大的数据利用价值。

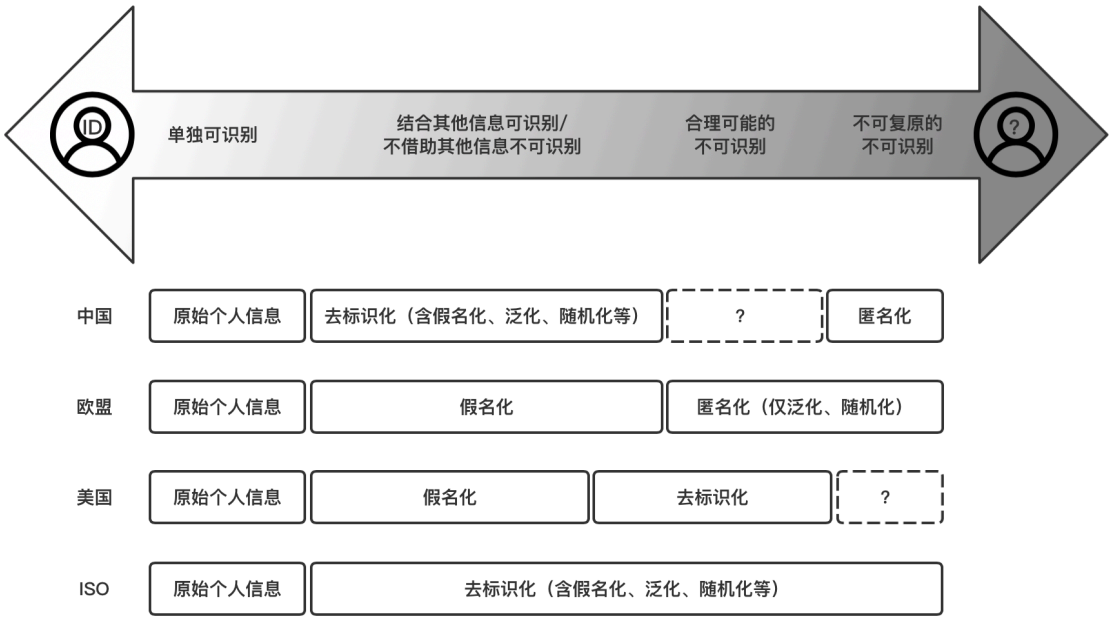
“数据脱敏”专题文章将梳理匿名化、去标识化、假名化等一系列相关概念，分析中国、欧盟、美国等法域对不同概念的法律评价，介绍数据脱敏的技术方案与隐私模型，探讨各个业务场景下的行业实践案例与法律落地方案，以推动数据利用和隐私保护的平衡发展。

“数据脱敏”专题往期文章链接

- 数据脱敏1 | “数据脱敏”是一个法律概念或技术概念吗？
- 数据脱敏2 | 不同法域下匿名化、去标识化、假名化的含义一致吗？
- 数据脱敏3 | 脱敏技术与法律效果评价可以机械对应的吗？
- 数据脱敏4 | 法律可以量化评价数据脱敏的效果吗？
- 数据脱敏5 | 数据脱敏的法律效果是渐进的吗？

上期回顾：对于脱敏效果的衡量，既有传统的定性标准，如第三人测试、黑名单制度，也有专门的定量标准，如K-匿名模型、差分隐私模型，为不可识别程度的量化提供了数学的工具。

既然脱敏处理后的不可识别程度是渐进的，按照义务与风险相适应的立法原则，数据脱敏的法律评价也应当是渐进的。但现行法下，个人信息和匿名化的法律地位较为明确，而对于过渡地带的去标识化信息，立法者仍然在探索过程中。本文将介绍并分析数据脱敏在各法域的效果评价。



注：括号内的概念为技术手段，括号外的概念为效果评价。

一. 无法识别：不再属于个人信息

在各国的现行法下，经技术处理而无法识别特定自然人的信息，不属于个人信息，因此不受个人信息保护的相关法律规制。

欧盟采用匿名化的概念，对于那些采用了所有合理可能的技术手段仍无法识别个人的匿名信息，不受《通用数据保护条例》（GDPR）管辖。

美国《加利福尼亚州消费者隐私法案》（CCPA）采用去标识化的概念，对于那些无法合理识别出个人的去标识化信息，不属于CCPA的个人信息范畴；《加利福尼亚州隐私法案》（CPRA）和《健康保险流通与责任法案》（HIPAA）同样排除了去标识化信息。

我国采用匿名化的概念，经匿名化处理后的信息不属于个人信息。《网络安全法》第42条和《民法典》第1038条在对个人信息的规定中设置了但书，“但是经过处理无法识别特定个人且不能复原的除外”。《个人信息安全规范》《个人信息保护法（草案）》更进一步明确，个人信息不包括匿名化处理后的信息。

此外，我国还在特定情形下将匿名化视为和删除相当的替代手段。根据《个人信息安全规范》，在个人信息超出存储期限、个人信息控制者停止运营其产品或服务、个人信息主体选择退出个性化的定向推送、个人信息主体为注销账户而提供身份核验信息等场景下，控制者应对相关个人信息进行“删除或匿名化处理”。

二. 结合其他信息可识别：非常有限的豁免

各国的现行法一方面为可识别的个人信息提供全方位的保护，另一方面解放了不可识别的信息。如果脱敏后的信息无法直接识别，但可以结合其他信息进行间接识别，则处于可识别和不可识别的中间地带，法律上往往缺乏明确的规定。

欧盟采用假名化的概念。由于假名化增强了信息的不可识别性、降低了风险，数据控制者应采取的安全措施水平也随之降低。例如，当发生数据泄露时，如果数据因采用加密等技术而无法被他人理解，则数据控制者可以免于通知数据主体。又如，如果数据控制者已经无法识别数据主体，且数据主体也没有提供额外信息，则数据控制者无须响应其访问、更正、擦除、限制处理、携带数据的权利请求。

美国采用假名化的概念，但没有设置专门的法律效果。

我国采用去标识化的概念，去标识化信息仍属于个人信息，原则上适用和个人信息相当的保护标准，享有的优待非常有限。此外，我国法上为个人信息处理者设置了去标识化处理的义务，并出台了去标识化技术的国家标准，但尚未给予去标识化以特殊的法律地位。

（1）非常有限的优待。《个人信息安全规范》规定，学术研究机构出于公共利益开展统计或学术研究所必要，在对外提供学术研究或描述的结果时，如果其对结果中的个人信息进行去标识化处理，则无需征得个人的授权同意；个人信息控制者共享、转让经去标识化处理的个人信息，且确保数据接收方无法重新识别或者关联个人信息主体的，则无需征得个人的授权同意。

（2）去标识化处理的义务。《个人信息保护法（草案）》要求处理者采取相应的加密、去标识化等安全技术措施。《个人信息安全规范》要求个人信息控制者在存储和展示个人信息时进行去标识化处理，并将可用于恢复识别个人的信息与去标识化信息分开存储、并加强访问和使用的权限管理。《个人金融信息保护技术规范》进一步要求，在共享、转让、委托处理、开发测试等使用去标识化处理的情形下，不应仅使用加密技术。

（3）去标识化的技术。国家标准《个人信息去标识化指南》详细说明了去标识化的目标与过程、七类常用技术、两种隐私度量模型。

三. 义务与风险相适应的立法路径

在我国现行法下，一方面，个人信息受到全方位的规制，保护了个人的隐私与安全；另一方面，匿名化信息被排除在个人信息之外，促进了数据的利用与流通；但是，法律尚未对去标识化信息进行差异化评价。因此，虽然数据脱敏所实现的不可识别程度是渐进的，但数据脱敏的法律效果却是断层的。

去标识化的法律空白导致了实践中的混乱。一方面，有的企业仅进行了最浅层的技术处理，就对外宣称自己使用的是脱敏数据，其实远远无法保护信息安全。另一方面，有的企业投入大量成本进行去标识化处理，却仍需要履行和个人信息相当的保护义务，白白折损了数据价值。

近年来，数据脱敏问题逐渐受到立法者的关注，我国已经在一些法律法规中提出了去标识化的特殊规定，也出台了专门的技术标准。在《个人信息保护法（草

案）》公开向社会征求意见后，诸多实务界人士也呼吁在新法中明确去标识化的法律地位，使义务与风险相适应，为企业应用数据脱敏设置激励。

关于去标识化的效果评价，立法上还需要考虑并解决一系列实际问题。例如，脱敏程度的衡量方式、重识别的主体范围、不同行业的特殊性、监管的落地方案等等。接下来的文章将结合不同行业的实践案例，探讨去标识化的可行路径。

本期小结与下期预告：我国现行法下，匿名化处理后的信息不再属于个人信息，因此不受个人信息保护的相关规制，但去标识化信息的法律地位尚不明确，引发了实践中的混乱。去标识化需要界定重识别的风险、考虑不同行业的特殊性、设计监管的落地方案，下期文章将结合实践案例，构想立法与执法的可能方案。