数据合规专题

第一期

数据处理者的保护义务

（2024 年 10 月）

数据合规管理工作关系到数据处理的合法性与正当性，与个人信息保护、企业稳定发展，乃至国家安全息息相关。只有更好地认识数据，才能深入了解数据处理工作的意义，从而做好数据全生命周期的合规管理。

本期内容旨在通过案例进一步明确数据处理者的保护义务。

【案例简介[1]】

2012 年 12 月 21 日，乐视网（天津）信息技术有限公司、乐视网信息技术（北京）股份有限公司（以下统称**“乐视公司”**）为证明陕西师范大学侵害其对《观音山》、《桃花运》、《疯狂的赛车》、《窃听风云》（下称**“影音资料”**）享有的信息网络传播权，委托韩俊芳在上海市徐汇公证处对其在陕西师范大学校园网浏览网页、在线播放和下载影音资料的过程及内容作了证据保全公证。

陕西师范大学认为，其已明确规定网站内部资源只供本校教职工使用且禁止外借账号，其他人员无权使用。乐视公司及韩俊芳均非陕

[1] 案例信息：（2021）陕 0113 民初 5074 号 陕西师范大学诉乐视网信息技术有限公司、乐视网信息技术（北京）股份有限公司等网络侵权责任纠纷案

西师范大学在校教职工,系在该校不知情的情况下,以非法手段入侵学校内网,侵犯其网络安全及数据安全,使学校承接的多项国家课题、科研项目存在泄密威胁,故以网络侵权为由将乐视公司及韩俊芳诉至法庭。

法院经审理认为,乐视公司在公证处证据保全的过程,系采取合理合法方式维护其合法权益的手段,且登录方式系通过陕西师范大学教职工账户及密码,访问陕西师范大学网站及资源的行为过程,不属于法律规定的“干扰、窃取”违法行为。乐视公司收集使用的相关数据为公证处证据保全的乐视公司版权资源,乐视公司使用相关数据目的合法,符合《中华人民共和国数据安全法》第三十二条第二款“应当在法律、行政法规规定的目的和范围内收集、使用数据”的规定。

同时,因陕西师范大学未能举证证明乐视公司获取VPN账户的方式,且乐视公司自述是通过校友获取,故无法排除校内人员泄露账户的合理怀疑,亦不能据此认定乐视公司私自掌握陕西师范大学内网登录方式即为侵权行为。乐视公司虽通过掌握陕西师范大学的内网登录方式获取证据,但其公证过程仅涉及“天坛FTP”“高清影音”板块而未访问涉密系统和涉密数据,且陕西师范大学亦可通过网络管理升级或要求持有密码的教职工等内部人员更改密码等方式进行网络管理,故不存在侵犯陕西师范大学的数据安全或存在相应威胁的情形。

因此,驳回原告陕西师范大学的诉讼请求。

【启示与建议】

上述案例中,由于陕西师范大学未能举证证明乐视公司采用非法

方式获取了教职工账户及密码并通过该等方式非法获取该校的其他涉密数据或信息，而乐视公司关于其通过校友获取该校网站账号和密码的陈述具有合理性，因而法院认定乐视公司访问该校网络的行为不属于法律规定的“干扰、窃取”违法行为。

虽然陕西师范大学主张其明确规定网站内部资源只供本校教职工使用且禁止外借账号，其他人员无权使用，但其并未采取有效的防范措施杜绝前述情况，因而产生了数据安全漏洞。

根据现行法律法规之规定，数据处理者负有以下数据安全保护义务：

1、取得数据处理的资质许可

根据《中华人民共和国数据安全法》第三十四条之规定，“法律、行政法规规定提供数据处理相关服务应当取得行政许可的，服务提供者应当依法取得许可。”

例如：经营基础电信业务，须取得《基础电信业务经营许可证》；经营增值电信业务，须取得《跨地区增值电信业务经营许可证》或《增值电信业务经营许可证》；从事经营性互联网信息服务，应当办理互联网信息服务增值电信业务经营许可证；应用程序提供者通过应用程序提供互联网新闻信息服务，应当取得互联网新闻信息服务许可，禁止未经许可或者超越许可范围开展互联网新闻信息服务活动；应用程序提供者提供其他互联网信息服务，依法须经有关主管部门审核同意或者取得相关许可等。

2、一般数据处理者的保护义务

（1）建立数据安全管理制度、开展数据安全教育培训。开展数据处理活动应当依照法律、法规的规定，建立健全全流程数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，保障数据安全。

（2）数据处理活动符合社会公德伦理。开展数据处理活动以及研究开发数据新技术，应当有利于促进经济社会发展，增进人民福祉，符合社会公德和伦理。

（3）加强数据安全等风险监测。开展数据处理活动应当加强风险监测，发现数据安全缺陷、漏洞等风险时，应当立即采取补救措施；发生数据安全事件时，应当立即采取处置措施，按照规定及时告知用户并向有关主管部门报告。

（4）不得窃取或以其他非法方式获得数据。任何组织、个人收集数据，应当采取合法、正当的方式，不得窃取或者以其他非法方式获取数据。法律、行政法规对收集、使用数据的目的、范围有规定的，应当在法律、行政法规规定的目的和范围内收集、使用数据。

（5）配合公安机关、国家安全机关调取数据。公安机关、国家安全机关因依法维护国家安全或者侦查犯罪的需要调取数据，应当按照国家有关规定，经过严格的批准手续，依法进行，有关组织、个人应当予以配合。

3、特殊数据处理者的保护义务

（1）利用互联网等信息网络开展数据处理活动的数据处理者：

利用互联网等信息网络开展数据处理活动的数据处理者应当在网络安全等级保护制度的基础上，依照法律、法规的规定建立健全全流程数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施以保障数据安全。

（2）重要数据的处理者：

重要数据，是指特定领域、特定群体、特定区域或达到一定精度和规模的，一旦被泄露或篡改、损毁，可能直接危害国家安全、经济运行、社会稳定、公共健康和安全的数据。

重要数据的处理者应当明确数据安全负责人和管理机构，落实数据安全保护责任；应当按照规定对其数据处理活动定期开展风险评估，并向有关主管部门报送风险评估报告。风险评估报告应当包括处理的重要数据的种类、数量，开展数据处理活动的情况，面临的数据安全风险及其应对措施等。

（3）关键信息基础设施的运营者：

关键信息基础设施，是指公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域的，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统等。此类运营者的保护义务在《关键信息基础设施安全保护条例》中有详细规定，与分会成员业务关联不大，此处不再赘述。

（4）从事数据交易中介服务的机构：在提供服务时应当要求数据提供方说明数据来源，审核交易双方身份，并留存审核、交易记录。

数据安全保护义务是数据处理者的法定义务，是数据合规的重要组成部分，数据处理者应当根据数据类型建立相应的数据安全及保护体系，以确保数据处理的合法性及正当性。

北京道商律师事务所

2024 年 10 月 21 日