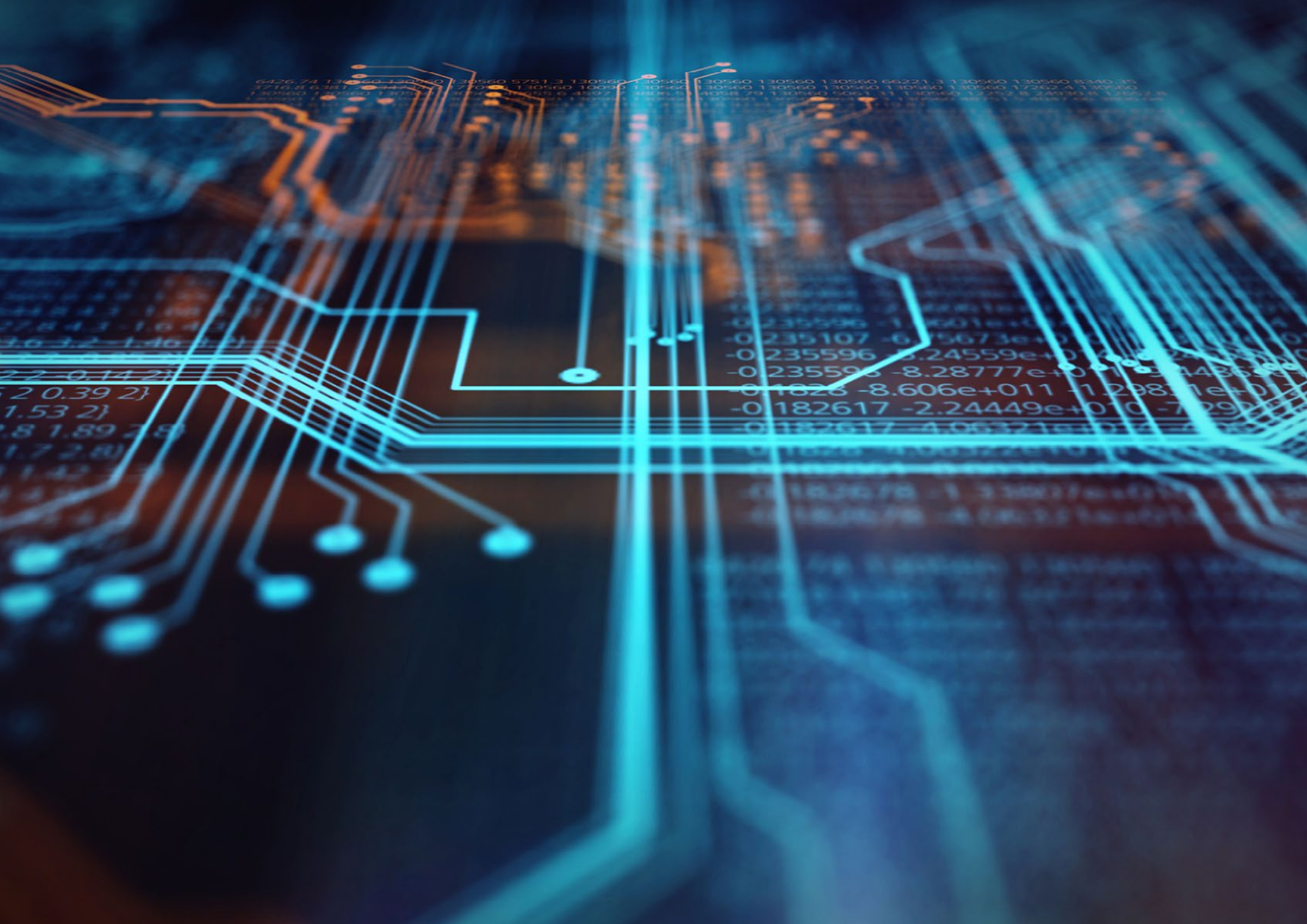




大成 DENTONS

市场洞察 数字化转型与数字消费者



前言

网聊、网购、在线观影以及在线听歌现已成为十分常见的在线活动。面对这些可能已经司空见惯的在线活动，企业必须适应新消费者行为、新竞争对手和新商业模式，而这对于它们而言并非易事。银行难以吸引年轻客户，因为相比于通常需排队等候的线下网点，他们更喜欢网上银行或支持快速贷款的移动应用程序。旅行社无法继续指望顾客去展销橱窗寻找新的旅行优惠。电视广播公司意识到传统线性免费电视的好时光已经不复存在。

第一股数字化转型浪潮首先席卷技术、媒体和电信行业，并且自然发展。有迹象表明此轮转型并未结束，而只是刚刚开始。其他更为传统的行业会很快面临变革，并一直延伸到大众媒体、电信和快速消费品行业。这股新浪潮会彻底摧毁一些企业（例如百科全书出版商），并使其他企业如同音乐公司一样发生巨大变革。

一些传统企业不愿意进行变革，这不足为奇。许多企业采取观望态度，首先了解竞争对手的举动，然后再决定是否采取行动。鉴于数据保护、安全和劳动法等因素，许多欧洲企业采取逃避做法，这种做法我们可以理解，但是似乎很快就会结束。毫无疑问，欧洲经济即将开启新技术革命，各个公司必须进行转型，抓住数字化转型带来的巨大机遇。

什么是数字化转型？

数字革命将改变传统公司的营商方式。这意味着各个公司须采用新技术解决方案并学习新技能，例如处理社交媒体和新兴物联网所产生大量数据的能力。

管理层必须巧妙地与新一代数字客户进行合作，提供最新数字应用程序和服务，并解决新的法律问题。选购技术只是企业实现数字化的开始。改变公司文化同样重要，而这往往更难实现。

什么是数字化转型？

数字化转型可概括为数字技术引发的变革，该等数字技术

- (1) 创造新的营销和沟通渠道及工具，
- (2) 提高公司运营流程的效率，
- (3) 增强客户体验，并/或 (4) 促进新业务模式的发展。

我们如今所处的状况？

大多数企业都意识到必须进行数字化转型，相关研究清楚地表明数字化转型非常有必要。Dell EMC 委托进行的 2017 年企业战略集团研究表明，71% 的受访者认为 IT 基础架构转型对于企业长期竞争力至关重要。但是，只有 5% 的企业处于 IT 成熟阶段，即“已转型”，这类企业是 IT 资源的活跃用户，它们将 IT 资源用于加速创新产品的开发、实现自动化流程，并将 IT 部门转变为利润中心。该研究显示，已转型集团中 96% 的公司已超过其收入目标。

2018 年 IDC 预测称，从数据中盈利以及从数字化中提高利润水平将成为 75% 首席信息官的首要任务。

企业通常面临的最初挑战是如何管理公司内部的变革。在最近的一项研究中，贝恩公司指出，有效的数字化战略必须结合一系列坚定的短期举措以及对创新如何改变整个行业的大胆设想。

多个行业受到冲击

法律市场也受到这种变革的影响。Dentons（大成）不仅了解企业面临的挑战，我们律所内部也在应对这些挑战。我们认识到客户对数字时代和二十世纪法律服务的期望不同。

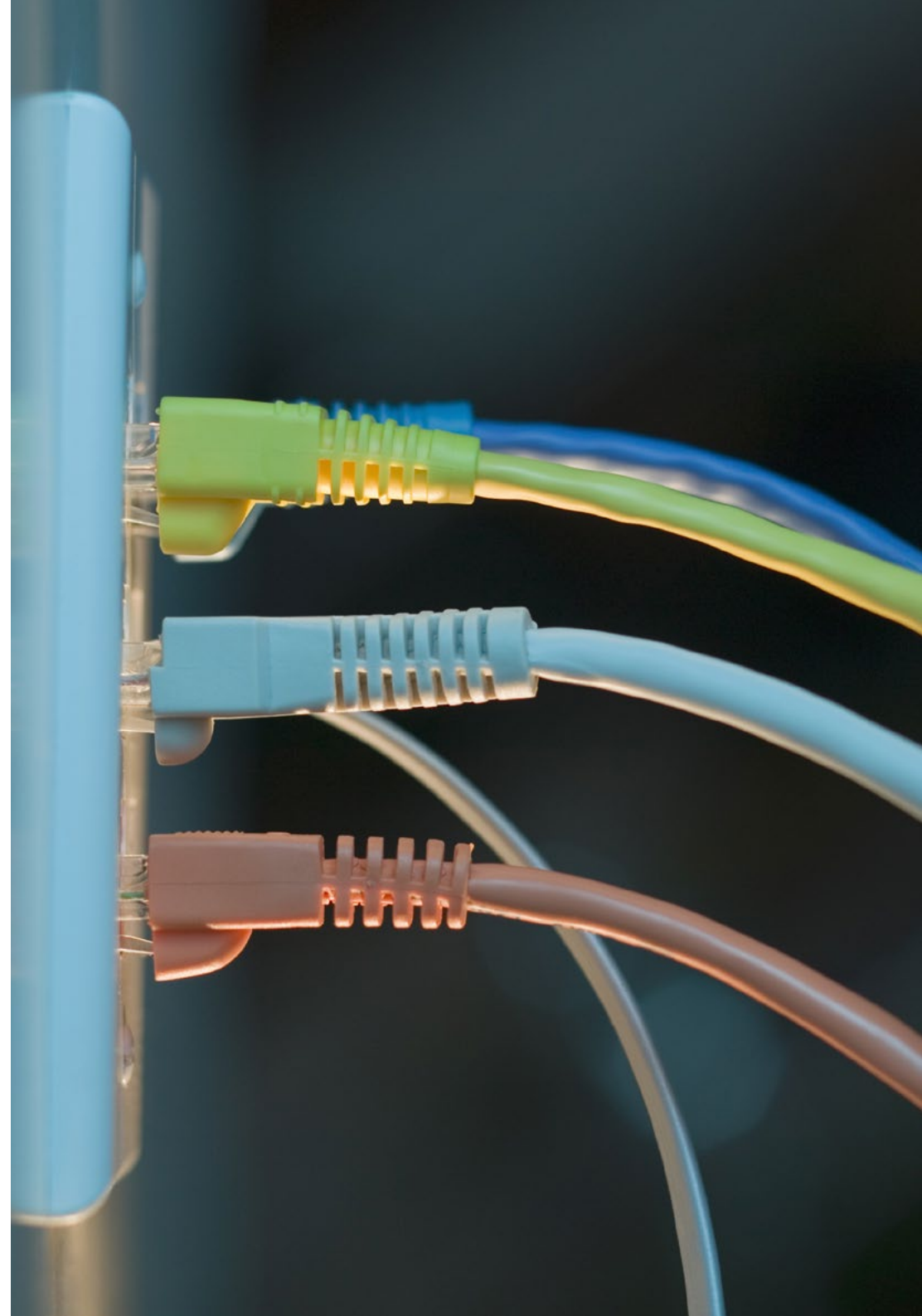
通过 NEXTLAW LABS 和 NEXTLAW VENTURES 创新法律实践

法律行业尚未如同其他专业服务行业一样从技术中获益。DENTONS（大成）正通过 NEXTLAW LABS 和 NEXTLAW VENTURES 改变这种状况。

NEXTLAW LABS 是由律师事务所成立的首家法律技术企业，由 DENTONS（大成）在 2015 年推出，旨在通过技术重塑法律业务和实践，并主导和塑造正在改变法律行业的颠覆性力量。利用独特的洞察力、有形产出以及世界上最大的律师事务所作为试验场所和支持者，NEXTLAW LABS 具备独特的优势，从而成为法律创新垂直市场的全球情报中心。

NEXTLAW LABS 以解决方案为导向，以客户为中心，它加速和推出领先的技术解决方案，孵化创新理念，进而开发变革法律服务业的产品和流程。它为 DENTONS（大成）及其生态系统提供“创新即服务”咨询，从而为实验、参与和协作提供安全沙箱。

NEXTLAW VENTURES 是一家在全球范围内活跃并专注于法律技术的早期风险投资企业。它目前的投资组合包括十家创新法律科技公司。NEXTLAW VENTURES 通过 DENTONS（大成）的法律人才、无与伦比的全球布局和广泛的客户群来协助发展其投资的公司。



维持安全

首先，我们了解，对公司而言，数字化意味着必须为将来使用的产品获得一整套商品、服务和许可证。如果实施的任何解决方案遭遇失败，需要解决在法律方面如何维持安全这一问题。此外必须牢记一点，数字消费者更有可能对侵犯其权利的任何行为作出反应，而雇员需要了解变革的内容。

这些问题将在本《市场洞察》中详细讨论。以下是对所讨论主题的介绍。

1 <https://www.emc.com/collateral/analyst-reports/esg-dellemc-it-transformation-maturity-report.pdf>

2 <http://www.bain.com/publications/articles/digital-strategy-for-a-b2b-world.aspx>

A close-up photograph of a hand typing on a computer keyboard. The image is heavily blurred, focusing on the motion of the fingers. A semi-transparent teal overlay covers the bottom half of the image, where the text is located.

与数字消费者保持同步

IGOR OSTROWSKI, 华沙

客户就是上帝

有一点是绝对可以肯定的：数字化标志着客户关注的新时代的到来。客户可以从社交媒体、在线评论、博客、聊天室和特定任务应用程序获得有关产品和服务的各种信息。他们通常由此知晓正在寻找的内容。

但是，这并未表明可以轻松地对每个数字客户进行分类。一些客户具有更强的意识，而其他客户的视角相当有限（例如他们可能会乐于通过其移动设备快速购买）。最后，有些人不知道如何安全有效地浏览信息或者如何识别值得信赖和诚信的供应商及服务提供商，因此仍感觉数字世界不安全。这些客户类型经常发生重叠，许多客户表现出不同分组的特征。在数字世界中构建客户关系时，我们应该牢记这一点。

随着数字技术的发展，客户的期望也在不断演变。爱立信《2018 年 10 大热门消费趋势报告》表明，超过一半的现有智能语音助理用户认为我们将通过肢体语言、语调、触摸和手势与技术进行互动，如同我们与他人的互动方式一样。三分之二的人认为在未来三年内这将会成为现实。在该项研究中，多达 30% 的受访者称新技术需要他们具备新技能。46% 的受访者称互联网使他们比以前更快地学习和忘记技能。

电子商务消费者权利

与上述内容相一致的是许多企业家发现电子商务中的机会。这一点不足为奇，因为网上购物呈现爆炸式增长，持续改变零售市场。政府当局已就此作出应对，即采取措施保护交易中通常处于较弱地位的电子商务消费者。

例如，欧盟成员国必须将消费者权利指令 (2011/83/EU) 纳入其法律体系。其中包括客户可在 14 天的冷静期内选择退出远程合同，并且当他们退货时，交易商通过其提供的成本最低的送货方式承担运费。

立法者还希望确保在达成交易之前，客户了解其必须支付的所有费用。卖方必须明确告知客户签约产生的所有费用，并禁止对信用卡付款和客户电话收取过多的额外费用，并禁止在购买的商品价格中自动纳入额外服务。另外还禁止使用误导性在线优惠，即错误地暗示商品或服务免费，而实际上客户仍须为此种优惠支付费用。

卖方有责任向客户明确告知其标识数据。网店网站必须显示公司名称、邮政地址、税号和电话号码等详细信息。另外还必须向客户提供取消表格以及如何取消合同的说明。第五章和第六章将更详细地介绍消费者保护和合同问题。

金融科技 - 最新前沿

随着金融服务行业技术不断发展，金融科技迅速成为新的前沿领域，各国政府正努力应对关键细分市场的数字化发展。随着金融科技创新的不断发展和演变，它们将继续改变公司的面貌。在第七章中，我们将探讨金融科技的发展、增长和创新，它处于严格监管的金融服务和数字创新之间的交叉点。

迈向数字单一市场

在欧盟运营的企业需记住，布鲁塞尔仍致力于制定有关数字单一市场的原则，这些原则奠基于消费者和企业自由获得商品、数字服务和网络以及促进数字经济和社会发展。这涉及通过 35 项法案，其中有几项业已得到实施。欧盟委员会称，如果建立并运行完全统一的数字市场，则欧盟每年可获利 4,150 亿欧元。目前的情况是各成员国间不同且复杂的增值税法和版权法等（约 80 种不同的法规）正在阻碍该进程。

目前迫在眉睫的是制定有关数据自由流动的法律草案。为了从欧盟数字经济中充分受益，欧盟委员会还拟定一套关于非个人数据自由流动的新条例。欧盟委员会主张各成员国不应期望各组织只在其地域内存储或处理数据。只有在涉及公共安全的合法基础上方可合理地施加限制。

成员国须将有关数据位置的任何最新或当前要求告知欧盟委员会。非个人数据的自由流动将使跨境业务运营更为容易并降低成本，而无需复制 IT 系统或者在不同地点存储相同的数据。随后制定欧盟良好实践准则，借此消除在更换云服务提供商以及将数据存储或传回用户的 IT 资源时面临的障碍。

这些变化旨在鼓励企业更乐意使用云服务，并且有信心进入新市场或者将内部 IT 资源转移到成本更低的地点。归根结底，欧盟委员会估计这将促使欧盟的 GDP 每年额外增加 80 亿欧元。第九章将更详细地介绍大数据问题。

谨慎处理（数据）

在与数字客户建立关系时，对数字数据（尤其是个人数据）进行适当管理是首要任务。《通用数据保护条例》(GDPR) 已于 2018 年 5 月 25 日在所有成员国生效。该条例引入一系列重大变化，包括在制定解决方案时需考虑数据保护要求，以及需保证只可在达到既定目标所需的范围内处理个人数据。新条例取代所有成员国此前实施的个人数据保护法。

在此前只可由监管机构实施处罚，但是根据新制度，消费者可直接向法院提起诉讼。不满意的客户、雇员和竞争对手很可能采取该行动。

各组织使用有关个人数据处理的一些法律依据时，应遵守更严格的条款，例如征得数据主体的同意。《通用数据保护条例》为个人提供广泛的权力，例如被遗忘权利和数据可移植权利。另外还扩大敏感数据的清单，现已包括生物识别和遗传数据。

因此，公司和机构在处理个人数据方面必须更加透明。它们必须向数据主体告知数据保留期等详情以及向监管机构提出投诉的权利。此外，如果发生任何数据保护违规，数据管理员必须在发现后的 72 小时内通知相关机构以及个人数据受到侵害的数据主体，并且必须妥善记录所有侵犯数据的行为，以便进行检查并确保实施适当的报告和记录。我们将在有关《通用数据保护条例》的第四章中对这些问题进行更详细的讨论。

除《通用数据保护条例》以外，正研究制定电子隐私条例，以针对互联网隐私引入更多的限制性法律条款。已规划制定的电子隐私条例的主要目标是保证电子通信所产生数据的保密性。这尤其涉及禁止非法干扰、窃听、存储或拦截数据。新法扩大电子营销的定义。

在新定义中，B2C 通信针对个人用户，而 B2B 通信针对公司。就 B2C 通信而言，须取得收件人的明确同意，方可向其发送消息。遗憾的是，对于向雇员进行的直接营销符合 B2C 通信还是 B2B 通信这一重要问题尚未作出明确回答，并且成员国可予调整，因此成员国之间可能继续存在分歧。

许多互联网广告公司对电子隐私条例所设定的措施感到担忧，例如显著扩大地域范围：向欧盟最终用户发送直接营销信息或者希望在最终用户设备上安装 cookie 的任何公司均须遵守电子隐私条例。第四章详细讨论使用数字数据的法律问题。在本指南发布时，电子隐私条例仍只有草案版本，可能会有所变更。

网络安全

对于越来越依赖互联网渠道和应用程序的企业而言，网络安全是一项挑战。去年，WannaCry 和 Petya 网络攻击引发大范围不良影响。WannaCry 是迄今为止最大的勒索软件，它封锁成千上万的设备，并危及英国国家健康服务、俄罗斯内政部、运输公司、电信和教育中心等系统。Petya 首先攻击乌克兰，后来扩散到俄罗斯及其邻国。它已攻击能源、运输和广告等各个行业的企业。

预计网络犯罪分子会改进其技术并提高攻击频率。在此背景下，思科创造出一种新型网络攻击术语：DeOS（破坏服务）。思科警告称，由于新攻击可能使目标公司完全丧失恢复数据或 IT 系统正常运行的能力，因此其比传统勒索软件的攻击更具破坏性。DeOS 使用破坏备份系统和支持网络的机制。随着物联网 (IoT) 和在线运营的日益普及，潜在的攻击目标数量正在增长，并可能导致前所未有的攻击升级。

以色列公司 Check Point 将此类攻击称为第五代网络攻击，它主要表现为多种环境之间的大规模和快速转移。它们能够绕过基于静态检测的传统保护系统，从而针对移动网络、云端和内部网展开复杂攻击。

但是这并不意味着无法阻止这些攻击。为了提高网络安全性，思科建议对 IT 系统和应用程序进行更新，以使网络犯罪分子无法利用任何已知漏洞，同时采用综合保护措施和可持续机制来积极应对安全威胁，并确保安全培训适于雇员的职务。从系统实施项目的早期阶段开始，网络安全就应当成为高级管理层的主要关注问题。关键是要采用明确方法来衡量和评估安全级别并简化网络安全实践。

第二章简要概括了不同类型的法律挑战，其中包括在成功实施数字化转型项目之前需要解决的网络安全问题。

我们应该信任数据中心？

云计算技术正在崛起。据华为称，到 2025 年，企业的整个 IT 基础设施将转移到云端，并且使用的 85% 应用程序将基于云服务，而目前比例仅为 20%。华为称所有公司的核心业务均将基于云计算技术，每家公司都会寻找最适合其需求的定制解决方案。

目前，许多公司（特别是金融公司）必须按照严格的数据保护要求开展运营，而这些要求极大地妨碍云技术的潜在应用。许多企业和机构倾向于安全运营，而不愿将客户或业务合作伙伴的数据存储在其物理位置以外的地点。另一方面，云服务提供商声称已获得符合数据安全和透明处理标准的证书。他们声称可确保在以下方面达到最高安全水平：数据存储；通讯；合作和文件共享；以及网站、应用程序和服务托管。

云端通过位于数据中心的服务器运行。在签订合同时，应当核实数据的存储位置并选择一家服务提供商，该提供商可保证在特定国家范围内所产生的数据按照该国法律受到保护。

建议检查数据中心提供的服务。尽管最初可能希望只使用一项或两项云服务，但是仍有必要选择提供不断发展的多种产品组合的提供商。当公司需要及时变革时，使用单个数据处理中心的服务更为方便。从单一提供商处购买的服务越多，议价能力就越大，相关安排的成本效益也越高。最佳方案是提供商能够按客户需求定制所提供的产品。第三章将介绍与数据中心相关的主要优势和挑战。

工作标准的变更

数字化不仅会彻底改变客户关系，还会影响所使用的工作标准。基于可用的 IT 解决方案，越来越多的人进行远程办公而非在办公室工作。在最后一章中，我们将介绍数字化对劳动法产生的一些重大影响。

德勤⁴最近发布的一份报告表明，雇主需重塑组织结构、人才管理系统和人力资源战略，跟上技术的步伐。公司雇员不仅仅是指资产负债表上所列的员工，还必须包括自由职业者、季节工、独立承包商和远程工人。但是，提高效率并非总是与技术进步密切相关。

德勤认为这源于人力资源部门不能紧跟不断变化的趋势，只有 35% 的人力资源专家认为其部门效率水平为“良好”或“优秀”，而只有 11% 的相关专家知晓如何创建符合未来发展需求的组织。

同时，Hays、Kinnarps 和 Skanska⁵ 联合编制的报告显示，受访者认为灵活性将成为未来几年劳动力市场的关键驱动因素。雇员希望能够选择工作时间、地点和工具。这对于年轻雇员而言尤为如此，他们习惯于多任务处理和频繁更换交付方式。该等重大变化对于需要应对不同时代雇员期望的雇主形成挑战。

由于远程办公对于许多雇主而言是新领域，他们需要考虑与这种劳动形式相关的新法律问题。例如，远程办公合同应规定工作规则，如何检查远程工作人员是否在工作（例如始终在登录状态）以及工作成果的发送方式。

重要的是，家庭办公和远程办公之间存在一定差异。两者均是指在家中或其他地点的雇员通过远程操作进行工作，但区别在于远程工作是定期进行，而家庭办公只是偶尔进行，并由雇员决定是否以及何时通过远程工作。

所有这些因素均会严重影响有关工作时间的法律规定，即我们在第 10 章中讨论的问题。雇员在晚上如何处理来自上级的电子邮件，这个方面也可能产生问题。

是否侵犯雇员的充分休息权？欧盟法院经常指出，雇主不得在雇员的业余时间向其施加任何义务。

随着智能手机和平板电脑日益普及，越来越多的雇员愿意在工作中使用自己的便携式设备。

一方面，接受自带设备 (BYOD) 安排的公司可通过更佳团队协作和雇员满意度来提高生产力。另一方面，这给企业带来新的挑战。保护公司及其雇员的机密数据免遭未经授权访问是首要任务。IT 部门需要为各种移动平台提供技术支持。通常来说，最困难的是让雇员愿意接受他们严格的安全规则。

一般来说，允许外部硬件连接到其网络的公司首先应制定合理实用的安全策略。此外，必须编制最新版清单，罗列使用内部网的设备以及具有访问权限的指定用

4 <https://www2.deloitte.com/content/dam/Deloitte/global/Documents/HumanCapital/hc-2017-global-human-capital-trends-gx.pdf>

5 <https://www.skanska.pl/4a29ca/siteassets/oferta/biura/raporty-i-standardy/raport-nie-boj-si-activity-based-working/nie-boj-si-activity-absed-working-raport-2017-ahys-kinnarps-skanska.pdf>

户。IT 团队还应制定数据存储规则，并规定是否可以将数据下载到移动设备上或者将其传送到办公室外部。有必要制定程序，以便在数据被盗或劳动关系终止时清理或保护数据。

机器人带来的挑战

人工智能已迅速成为日常生活的一部分，在第 11 章中我们探讨人工智能的发展。雇主和雇员可能很快就会面临使用机器人带来的挑战。2017 年德勤报告⁶显示，53% 的受访者已开始实施机器人和自动化流程，另有 19% 的受访者计划在未来两年内如此行事。根据该报告，机器人最终可取代五分之一的全职雇员，同时增加收入。64% 的管理人将机器人流程自动化 (RPA) 视为企业宏观战略计划的一部分，并且大多数人认为机器人流程自动化的投资在不到 12 个月的时间内即可实现收支平衡。因此，未来公司寻找的雇员可能与现有雇员具有不同能力。

目前尚无法充分预测数字革命以及使用人工智能或虚拟现实等技术带来的影响。在与 Dentons（大成）合编的人工智能报告中，Polityka Insight⁷ 强调相关技术可通过使常规和耗时流程自动化来提升经济潜力，从而使雇员执行获利更高的任务。人工智能可提高不可替代雇员的生产力，同时降低资本成本，为增加经济投资开辟道路。资本成本降低对于存款储蓄较少的国家来讲至关重要，因为这可以让没有开发特别定制应用程序潜力的公司用上更多的先进技术。

但是，根据 SAS⁸ 最近的研究，32% 的 EMEA（欧洲、中东和非洲）受访公司表示，与使用人工智能相关的道德问题是人工智能技术使用方面的主要挑战之一。受访者还指出，面临的主要挑战包括责任问题（包括法律责任）、人工智能无法对其行为做出道德判断，以及人工智能的潜力被高估。

SAS 专家强调称，人工智能没有创造或创新能力，缺乏人类的直觉或理解力。这些人类品质使我们能够区分好坏，并理解模糊信号。没有这些技能，人工智能系统可能遭到故意提供虚假数据和破坏认知过程的人操纵。2017 年初，欧洲议会通过了一项关于机器人和人工智能操作法律责任的决议。欧洲议会议员呼吁欧盟委员会考虑成立欧盟机器人和人工智能机构，从而在技术、道德和法律领域为公共当局提供支持。

我们确实生活在有趣的时代，并且可以预期在不久的将来会见证更多变化，其中包括有关人工智能的规定。因此，本文并非旨在提供有关数字化转型的综合指南，而是提供开放性选项，其中探讨新主题并随着市场发展增设新章节。

⁶ <https://www2.deloitte.com/content/dam/Deloitte/pl/Documents/strategy/deloitte-es-consulting-robots-are-ready.pdf>

⁷ https://www.politykainsight.pl/en/_resource/multimedia/20145296

⁸ https://www.sas.com/pl_pl/news/informacje-prasowe-pl/2018/sztuczna-inteligencja-nie-rozumie-ludzkich-emocji.html
<https://www.sas.com/sas/offers/17/the-enterprise-ai-promise.html>



入门指南 - 为转型项目扫除法律障碍

MARC ELSHOF, 阿姆斯特丹

为了成功实施和执行数字化转型项目，需解决许多法律问题，其中包括：传统 IT 系统、合同、数据处理、网络安全、知识产权和监管。在项目的早期阶段解决这些法律问题有助于避免代价高昂的延误，并防止向客户提供的服务发生中断。

传统 IT 系统

根据定义，许多数字化转型项目旨在使传统 IT 系统现代化，以将更好地满足公司及其客户的未来需求。这通常意味着公司需采购新的硬件和软件，这些采购项目通常占项目预算的很大部分。通常来说，数字化转型包括将现有软件产品的许可证与定制软件组件的开发相结合。

在启动数字化转型项目之前，一定要检查现有的许可证和维护合同。是否可以终止现有合同，如果“是”，那么终止成本是多少？是否可以更新现有许可证，从而无需采购全新产品？合同中是否载有任何退出协助安排？

同样重要的是要牢记，数字化转型产品通常与其他软件和/或数据库相关联。在启动项目之前，请考虑成立一个整合团队来监督转型项目每个阶段的采购、推广、整合和法律因素。

与合作伙伴签约

如果数字化转型项目未取得成功，购买的昂贵软件通常只有很少的用处，甚或根本没有用处。通常来说，项目的各个组成部分应交由多个提供商处理。这可能会产生一些问题：如果其中一个合同（例如开发合同）未予执行，但是单独许可的标准软件可妥善运作，则公司打算如何处理？我们是否有义务继续使用过时软件？如果定制插件的开发合同终止，我们是否可以继续使用特定的标准软件？至关重要的是在一开始就确定如果一个合同终止，则对其他所有合同会产生何种影响。

软件和数据库产品之间通常存在高度关联性，因此，至关重要的是不仅要确保技术组件的互操作性，还应确保合同框架的统一。这意味着应签订内容明确的合同服务水平协议（包括义务和责任的划分），从而避免在这些合同间留下空白之处。包括法律部门代表在内的“数字整合”中心团队可负责监督和协调项目的各种采购活动。

但是，采购标准软件通常不是法律部门最难解决的问题。相反，定制软件的开发合同通常会带来最大的失败风险。

敏捷软件开发协议通常被设定为服务合同，并且未明确规定开发人员的义务，例如可交付成果、时间表、处罚、合作责任和知识产权转让。这种方法可导致严重延迟或项目失败，并且公司不可要求强制执行。因此，在起草开发协议时应始终保持谨慎，并考虑到具体情况和项目的可交付成果。

数据处理

数据聚合和组合是许多数字项目的关键职能。但是，复杂且不同的数据保护条例和数据所有权问题可能会限制公司实施这些关键职能的权利。为了成功解决数据处理带来的挑战，需采用三种方法：

- 清楚地了解相关的隐私和数据保护框架
- 分析数据流和法律框架
- 创建并在后续实施法律、组织和技术解决方案（例如匿名化或假名化）。

随着欧盟《通用数据保护条例》(GDPR) 的实施，数字化转型项目的一个关键方面是考虑数据泄露问题以及应对方法。在第四章中，我们更详细地探讨《通用数据保护条例》带来的影响，包括欧盟和非欧盟业务需考虑的因素。

网络安全

在当今的经济环境中，雇员需要从多个设备即时访问来自不同位置的数据。云端解决方案愈加盛行，成为具有成本效益、安全且灵活的数据存储形式。在下一章中，我们将详细介绍数据中心和云端解决方案，包括欧洲数据中心部门的持续增长。

但是，将数据放在网上意味着其面临网络攻击的风险更大。这些重大风险包括对声誉、业务中断、诉讼、知识产权损失和机密信息的潜在损害以及监管处罚。最重要的也许是由于网络攻击通常针对敏感的客户数据，当存在安全漏洞时，可能损害客户对公司业务的信任，有时这甚至是不可挽回的。

为了缓释这些网络安全风险，需要采取积极和综合的预防措施来避免、备战和应对网络攻击。这需要公司各个部门之间的密切合作，以了解、检测和响应这些先进和不断演变的威胁。

知识产权

知识产权是任何数字化转型项目的关键方面。正如第八章所述，知识产权保护允许创造者从其工作中受益，同时所有者从其对创造活动的投资中受益。但是，尽管知识产权法律有助于保护和促进原创性、创造性和创新性，但是技术进步也可以助长侵犯知识产权的活动。

首先，需要确保公司有权将软件用于预期目的。这可能包括扩展和减少许可证的安排。

但是，作为数字化转型项目的一部分，需要考虑如何最好地保护公司知识产权。数字技术使得分享创意和内容变得越来越容易，但是对于知识产权的界定却不是很清楚。

知识产权保护框架因司法管辖区而异，并且相关法规未必都适用于数字世界。这可能给知识产权管理及后期的商业化带来挑战，特别是在开源环境中创造的技术/创意或者来自不同方的信息。我们在第八章中探讨在面对颠覆性技术时如何应对和保护知识产权。

监管框架

在银行、保险、医疗保健和公共服务等受到高度监管的领域，需要密切监控适用的监管框架。由于适用规则快速发生改变，并且往往分散于国家或超国家层面的不同法律来源，因此这可能构成一项挑战。

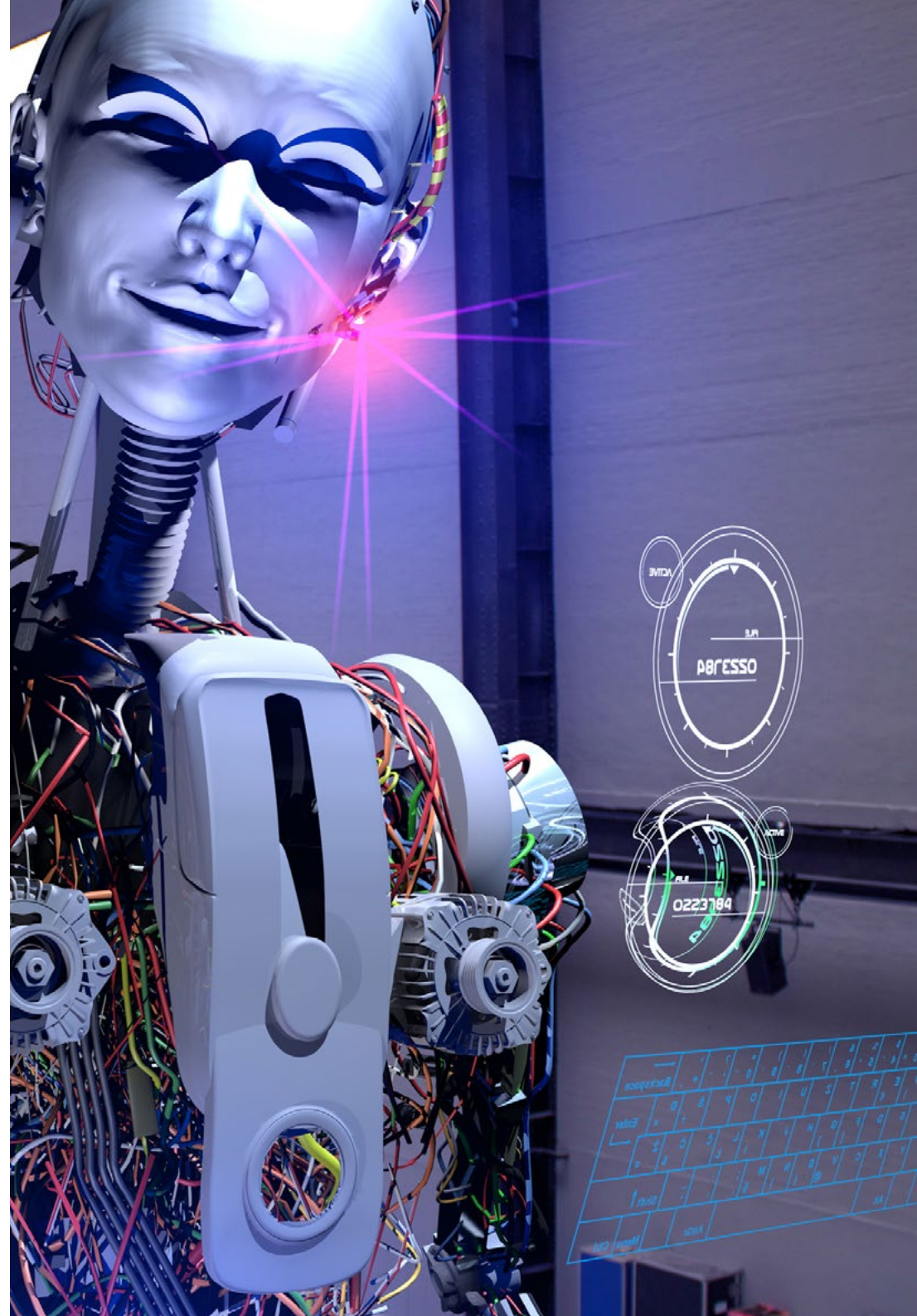
例如，无人驾驶汽车的出现给立法者和监管机构带来必须回答的一些问题。如果发生车祸，由谁负责？谁承担责任？司机？汽车制造商？软件开发人员？

随着法律框架的发展和新规则的实施，需要持续调整公司政策以维持其最新状态并符合法律。

如果数字化转型战略涉及启动最新数字平台或技术，应当尽早进行全面的风险评估，以识别和减轻使用该技术可能给客户带来的任何潜在威胁或危险。这种谨慎做法不仅可以帮助建立和维护与客户群的信任关系，还可以帮助在产品推出后最大限度地减少额外的监管负担。

总结

在项目早期阶段就考虑和规划这些法律挑战可帮助避免潜在隐患和高成本延迟。要做到这一点，重要的是组建一个由跨部门（包括法律、IT、风险管理和采购部门）关键人员组成的数字团队，确保公司在启动数字化转型项目之前奠定坚实的基础。





数据中心 - 欧洲云端和主机托管市场的中心

CHRISTOPH PAPENHEIM 和 SVEN-OLIVER FRIEDRICH, 法兰克福;
SHANE MERCER, 多伦多

作为公司数字化转型战略的一部分，创建数据中心是最常见的项目之一。将 IT 服务集中到最先进的数据中心或云端可以带来许多优势，包括节省成本、提高效率、减少重复和提高 IT 安全性。对于国际企业而言，在战略地点设立区域数据中心可以为遍布全球的办事处提供 7*24 小时的 IT 支持，改善客户服务。

欧洲的数据中心服务市场因此出现快速增长，无论是数据中心即服务 (DCaaS) 还是基础设施即服务 (IaaS)。法兰克福、伦敦、阿姆斯特丹和巴黎是欧洲数据中心最受欢迎的地点，主要原因是它们靠近大型金融市场。这些地点还提供完善的基础设施以及对领先互联网交换机的直接访问，如法兰克福的 DE-CIX、阿姆斯特丹的 AMS-IX、伦敦的 LINX 和法国巴黎的 IX。

自建、外包或购买？

在建立数据中心时，有三种主要策略可供选择：

- 自建数据中心
- 外包给传统的数据中心或云提供商
- 购买现有的数据中心

选择何种策略取决于自身业务的需求和能力。

例如，大公司对数据处理的需求量大并具备 IT 专业知识，因此可运营自建数据中心且相关成本在可接受范围内；而小公司则最好进行外包。快速发展的公司可能更倾向于云端解决方案，因其具有灵活性和可扩展性。某些公司如果持有客户的非常敏感数据，则可能倾向于运营内部数据中心，以便直接控制该等数据的位置和处理。无论选择哪种策略，都将面临法律挑战。下文将详细讨论这些主题。

建立数据中心

房地产

在建立数据中心时，有很多关于位置的考虑因素。根据业务规模和复杂程度，可以考虑利用现有场地来管理引入其他资产的成本或降低复杂度。在进行选择时需考虑许多因素，包括成本、复杂性、关联性、权力、管辖权、区划、可用人才、可访问性、稳定性、税收以及外部风险或影响（例如内乱和自然灾害风险）。

如果企业位于数据中心附近，则可减少连接等费用，但是可能需自行承担场地和公用设施的额外费用。另一方面，将数据中心设在更偏远的地点则可节省场地费用，但是会增加电信或差旅费用。这可能是一个具有长期影响的困难决定。在评估时寻求帮助可能会带来益处，特别是在考虑潜在区划、税收、管辖权和其他法律影响时。

购买和租赁设备

一旦确定新数据中心的位置，就可以考虑着手建立。打造精心设计的数据中心既昂贵又复杂，其中涉及的众多技术旨在提供强大的安全性、灵活上架、备用电源（UPS 和发电机）、冷却和连接。在决定购买或租赁所需的基础设施时，应考虑潜在的税务影响，（由于不断变化的业务需求或监管要求）随着时间的推移，自身要求的潜在变化以及每个选择的财务影响。可能会发现，相比于某种方法，基础设施的各个方面与另一种方法更为匹配。

安全和隐私

数据中心的物理安全性与系统安全性同等重要。至关重要的是清楚地了解法律和监管要求，确保能够满足或超过这些要求。在适当情况下，与第三方（例如维护提供商或数据中心员工）签订的合同协议中应包括解决责任问题的适当条款。工

作场所的物理设计也可能受到这些要求的影响，例如数据中心内部各区域间的划分或者安全系统和/或程序的引入。

人员配备

在为新的数据中心配备人员时，应考虑将内部员工和第三方支持结合起来。需要实施适当的背景调查，制定保密协议，并确保每个人都在一系列政策下按明确规定的许可用途进行操作。

至关重要的是确保雇用情况符合相关业务的特定当地法律和监管要求。在考虑第三方支持时，应实施风险评估，签订的协议应确保充分的法律覆盖范围，从而明确规定服务水平、责任和其他适用的法律考量因素。这些人员可能访问最敏感的数字资产，应予以相应制约。

外包给传统的数据中心或云提供商

数据所有权

当企业考虑将其数据和系统进行外包托管时，非常重要的是明确说明提供商对信息的访问权限。在许多外包关系中，提供商无权直接访问系统和数据。在其他情况中，提供商可更直接负责管理系统，并可访问基础信息。在任何情况下，重要的是应通过合同来加强对业务数据的所有权和其他权利。一些云提供商已建立基于信息货币化的业务模型，因此需要确保不会出于其他任何目的而无意地向提供商授予扩展权限。

服务水平协议

可以与不同的外包提供商协商服务水平以满足特定要求，这通常需增加费用。由于其他提供商是提供商业务模型的核心，并由整体客户群共享，因此可能无法与其协商服务水平。

对于许多提供商而言，服务水平取决于对平台技术能力的理解以及是否设计系统以提供高弹性服务。从本质上讲，如果未按要求正确设置系统，则会导致获得的保证失效！

数据位置

一种常见的误解是当企业将其数据中心外包给云提供商时，数据的实际位置不明确。与传统的数据中心提供商不同，大多数云提供商都能够明确说明信息存储位置，或者提供直接控制权。在选择提供商时，请务必清楚地了解如何存储系统和数据以及保留何种控制权。在适当情况下，还应确保在合同中规定相关限制，确保提供商平台上的未来变更不会对业务产生负面影响。不仅应仔细检查运行系统的存储方式，还应检查备份系统，包括备份数据。这些内容通常存储在不同的物理位置，甚或可能存储在其他国家/地区。

数据保护和隐私

无论外包安排的性质如何，数据保护和隐私都是企业和提供商的共同责任。可以通过外包提供商提供的功能来提高自身安全性，但这不会免除责任。同样，这取决于清楚地了解提供商的能力并设计系统加以利用。例如，如今大多数提供商在将数据存储在其系统上时进行加密。但是，也可以使用自己的“密钥”来加密数据。这种扩展能力可能成为是否满足某些监管要求的关键。

必须确保潜在提供商的能力符合独特业务的要求，并且可加以利用。

就数据隐私而言，清楚地理解与提供商所建立关系的性质以及他们对系统和数据的访问权限，对于了解义务如何扩展至他们也很重要。就《通用数据保护条例》等法规而言，这种了解至关重要。例如，如果提供商可以访问系统和基础数据，则可将它们视为数据“处理者”。如果他们无法进行这类访问，这可使他们免于

承担这些监管责任。任何合同协议中均应考虑与数据保护和隐私法规相关的特定法律要求。

无法提供服务或产生安全漏洞的责任

发生无法提供服务的情形（在更糟糕的情况甚或产生安全漏洞）几乎是不可避免的。良好规划和仔细选择符合要求的供应商将降低风险和减轻潜在影响，但是仍不能完全消除。在与提供商谈判时，应始终确保明确地界定和理解责任限制。应当获得保险证明并定期进行更新。还应检查自身是否投保商业险，明确保险范围足够。

数据可移植性和转换协议

与任何业务关系一样，始终应制定退出策略。在与外包数据中心或云提供商建立关系时亦应如此行事。提供商可能拥有一些最敏感数据，因此应确保在关系中断或者决定转换时得到合同的保护。

在转换系统和数据时，请考虑相关的潜在财务义务、时间承诺和流程。在建立关系时，请预先就这些棘手事宜进行讨论，并确保在合同中记录该等事宜，这有助于防止在将来发生潜在的敏感情形。

购买数据中心 - 并购考虑因素

资产交易或股票交易

通常有两种交易方式：资产交易、股票交易。在资产交易中，买方获得卖方的某些资产并承担某些责任。在股票交易中，买方通过其股份或权益获得业务，包括所有资产、负债、权利和义务。虽然选择哪种方式取决于交易情况，但通常是基于税收影响、复杂性和避免承担某些责任的期望来进行决策。数据中心交易通常采用资产交易的方式。

初步协议

在早期阶段签订初步协议（例如保密协议、意向书、谅解备忘录和条款清单），予以保密并列预期交易的关键条款和时间表。此外，买方可寻求一定期间的排他性。

尽职调查

为了更好地了解目标业务和识别任何潜在风险，谨慎的买方应进行尽职调查，重点关注法律、财务、税务、环境和商业领域。在购买数据中心时，法律尽职调查的重点将放在房地产上，特别是调查是否遵守公共建筑法。尽职调查还应关注目标主体与客户、提供商和其他业务伙伴之间的关系以及公司、税务和融资问题导致的合同问题。尽职调查还应检查是否符合数据保护和安全要求。

最终买卖协议

一旦双方商定交易的法律和商业条款，则将签订最终买卖协议。其中包括与出售相关的当事人陈述和保证、赔偿、契约和其他义务等条款。在某些情况下，买卖协议可能包括必须满足的条件才能完成交易，例如政府批准（如合并批准）、第三方批准（如关于合同关系的转移）或者豁免控制终止权的变更。

如果违反提供的保证，法律补救措施是获得损害赔偿金。就违反运营保证（例如合同、雇员、资产）通常设定损害赔偿的下限，就违反基本保证（例如资产或股份所有权）通常设定损害赔偿的上限（通常相当于购买价格）。

税收规划

税收结构是购买事宜中的关键因素，买方应在开始交易时寻求节税结构。在转让房地产时需缴纳房地产转让税。股票交易和资产交易通常免征增值税，只要后者涉及持续经营的整体业务或业务部门的出售。与目标及其获得的业务运营相关的税务风险，通常由采用特定赔偿和担保形式的买卖协议管辖。在资产交易中，谨慎的买方应排除资产或业务附带的任何类型纳税义务，并就承担的任何纳税义务寻求赔偿。

结语

建立高质量数据中心（无论是自建还是外包）是代表公司作出的重大投资和承诺。如果行事妥当，可为公司带来显著的成本和效率优势，同时确保为客户提供一致、稳定和可靠的服务。如果数据中心项目发生问题，可能对业务带来重大损害，并且不利于客户。

数据中心项目若要取得成功，需要 IT、法律和风险管理部门进行密切协作，以及作为内部客户的前线部门的积极参与。需要考虑 IT、法律和风险管理等多方面因素，因此我们强烈建议尽早就整个项目寻求法律和税务建议。





遵守不断变化的法规 - 《通用数据保护条例》

VICTOR NAUMOV, 圣彼得堡

在如今的便利型经济中，越来越多的人在网上购买商品和服务。每次购物都会留下数字足迹。随着时间的推移，这些足迹在网络空间积累，可用于确定身份。在这方面，保护个人数据和隐私是电子商务中保护个人权利的必要组成部分。

保护个人数据和隐私权

欧盟有关数据保护的主要法规是欧洲议会和理事会于 2016 年 4 月 27 日通过的第 2016/679 号条例《通用数据保护条例》，该条例自 2018 年 5 月 25 日开始在所有欧盟成员国实施。《通用数据保护条例》的目的是统一整个欧盟的数据保护法规。对于涉及电子商务的任何公司而言，熟悉这些新义务并投入足够时间予以遵守非常重要。

根据《通用数据保护条例》的规定，与可识别自然人（数据主体）相关的任何信息均属于个人数据。可识别自然人或数据主体是指可直接或间接识别的个人，特别是通过姓名、身份证号、位置数据、网上标识或者自然人所特有的一项或多项的身体性、生理性、遗传性、精神性、经济性、文化性 or 社会性身份信息。

《通用数据保护条例》是否适用于欧盟以外的国家或地区？

值得注意的是，就电子商务和个人数据而言，《通用数据保护条例》概述在数字世界里如何处理个人数据特定方面的一系列先进规则。

第 3 条规定《通用数据保护条例》适用于个人数据的处理，无论是否在欧盟地区进行此等处理。

除此以外，就以下两种情况而言，即使控制者或处理者不在欧盟处理个人数据，亦应适用《通用数据保护条例》：第一，如果控制者或处理者向位于欧盟的个人提供商品和服务，第二，如果它监控位于欧盟的个人。该等实体必须遵守《通用数据保护条例》。例如，他们需要在欧盟委任一名代表，以代表控制者或处理者履行其在《通用数据保护条例》项下的各自义务。

《通用数据保护条例》中规定的这两种域外效力尚须作出进一步澄清。如果控制者或处理者明确计划在一个或多个欧盟成员国提供商品和服务，则应视为该等控制者或处理者在欧盟提供该等服务。该等意图可通过在电子商务网站上使用欧盟语言或货币、欧盟客户订购商品和服务的可能性或者客户/用户位于欧盟予以证明。因此，如果只是可以在欧盟访问控制者或处理者网站、电子邮件地址和其他联系方式尚不足以确定该意图。

监控的定义也相当广泛，就《通用数据保护条例》而言，可以将其解释为使用各种技术机制来收集和分析数据以用于剖析个人。鉴于该等剖析行为的普及，开展在线业务的许多公司均应遵守《通用数据保护条例》。

隐私及其对剖析行为的影响

为了确定相关活动是否属于剖析行为，必须确定三个基本要素：

- 使用自动化处理方式；
- 包括个人数据的使用；
- 活动的目的是评估与自然人相关的某些个人因素，以分析或预测关于自然人的工作表现、健康、个人偏好、兴趣、位置或运动方面的信息。

个人有权不受只基于自动处理所作决定的约束，包括对其产生合法或其他重大影响的剖析行为。另外还必须将有关剖析活动的信息告知个人，该等个人有权不参与此类活动。

数据可移植性

应当注意的另一项个人权利是数据可移植性。这意味着个人有权接收他们此前以机器可读的常用格式提供的个人数据。但是，该权利受到限制，因为只有基于同意或合同来处理个人数据时方予适用。

合规挑战

数据保护和隐私是我们这个时代最具争议和挑战性的问题。电子商务公司（实际上包括在当今数字经济中开展运营的所有公司）的首要任务是遵守《通用数据保护条例》。

俄罗斯的个人数据保护

俄罗斯的个人数据法规在很多方面与《通用数据保护条例》相似：如果运营商建立以俄罗斯受众为目标的网站，则无论他们是否在俄罗斯设有当地代表，俄罗斯个人数据法律适用于该等运营商。由于“本地化修正案”规定公司有义务将俄罗斯公民的个人数据放置在俄罗斯，因此其具有相当大的影响力。

但是，俄罗斯法规采用稍微不同的标准来确定通过网站运营的外国运营商是否遵守俄罗斯个人数据法规。外国运营商是指：

- 使用与俄罗斯相关域名和/或俄罗斯原版网站的外国运营商；或
- 符合有“明确证据表明网站所有者计划将俄罗斯市场纳入其业务战略”之额外标准的外国运营商。这些证据可以包括使用卢布支付、向俄罗斯交付商品和/或使用俄罗斯广告转引至网站等。



A photograph of a person's hands using a credit card at a laptop. The person is holding a gold credit card over a laptop's trackpad. A pink cup of coffee is visible on the left. The image has a teal overlay at the bottom.

消费者保护和在线广告

和 TÜNDE GÖNCZÖL, 布达佩斯

由于通过互联网购买商品和服务的消费者数量持续飙升，电子商务业是当今经济中最具活力的行业之一。尽管电子商务为客户带来许多益处，例如易于访问、无限选择、优惠价格和便捷支付选择，但是也存在风险，其中包括支付欺诈、误导性广告和滥用个人数据等。为了降低这些风险，立法者开始保护电子商务消费者的权利。

消费者保护

在当今的全球商业环境中，企业应考虑电子商务的跨境性质及其目标市场的各种法规。尽管这似乎是一项艰巨的任务，但是主要的消费者权利和保护已通过欧盟指令进行统一，并与欧盟以外国家/地区的相关规定非常相似。

《电子商务指令》⁷直接规范电子商务业。此外，消费者保护和消费者权利受到欧盟《消费者权利指令》⁸、《不公平商业行为指令》⁹和《合同不公平条款指令》¹⁰的规范。这些指令中规定的大多数规则同样适用于线下和线上交易。电信公司必须进一步遵守《普遍服务指令》¹¹的规则，其中包括某些用户权利。此外，欧盟委员会正制定新规则以进一步加强对数字消费者的保护。

1.明确、透明且易于获取的信息

在电子商务中，当消费者无法看到或检测商品时，他们的信息权至关重要。因此，电子商务经营者应披露明确的信息以使客户能够就其交易做出明智决定。

在线运营的企业必须向其客户提供签约前信息。根据《电子商务指令》，在线企业必须提供有关企业的一般信息，包括公司名称、地理位置和联系方式（包括快速通信的电子邮件地址）。

此外，企业必须提供商业登记簿中有关其自身的详情及其注册号。如果公司的运营须取得授权，则必须提供授权详情。就受监管职业而言，应提供专业机构、职称和成员国，并提供相关的专业规则以供审查。

根据《消费者权利指令》，在数字领域运营的企业还须遵守其他要求。例如，必须列示商品或服务的主要特征，价格应当是透明的，其中包括运费、税款和其他任何费用。如果在签订合同之前无法计算运费，则应告知客户。在适当情况下，必须说明接受的付款方式以及预计的交货截止日期。

7 欧洲议会和理事会于 2000 年 6 月 8 日通过的有关信息社会服务（特别是内部市场中的电子商务）某些法律方面的第 2000/31/EC 号指令（有关电子商务的指令）

8 欧洲议会和理事会于 2011 年 10 月 25 日通过的有关消费者权利的第 2011/83/EU 号指令，修改欧洲议会和理事会通过的第 93/13/EEC 号指令和第 1999/44/EC 号指令，并废除欧洲议会和理事会通过的第 85/577/EEC 号指令和第 97/7/EC 号指令

9 欧洲议会和理事会于 2005 年 5 月 11 日通过有关内部市场中不公平的企业和消费者间商业行为的第 2005/29/EC 号指令，并修改欧洲议会和理事会第 84/450/EEC 号指令、第 97/7/EC 号指令、第 98/27/EC 号指令和第 2002/65/EC 号指令以及欧洲议会和理事会第 2006/2004 号条例（《不公平商业行为指令》）

10 理事会于 1993 年 4 月 5 日通过的有关消费者合同中不公平条款的第 93/13/EEC 号指令

11 欧洲议会和理事会于 2002 年 3 月 7 日通过的有关电子通信网络和服务的普遍服务和用户权利的第 2002/22/EC 号指令（《普遍服务指令》），经第 2009/136/EC 号指令修订

《不公平商业行为指令》规定若干额外要求，确保消费者在购买前获得完整和真实的信息。最重要的要求是向消费者提供他们作出明智购买决定所需的任何相关信息。该要求还包括数字设备上的技术解决方案，以使消费者可以决定是否使用数字服务。

《不公平商业行为指令》中的另一项重要规定是公司应概述其行为背后的商业意图。例如，在 Instagram 或 Facebook 等社交媒体平台上发布广告时必须说明广告性质。在针对不公平商业行为执行该等规则时，当局越来越关注社交媒体上的“意见领袖”。如果意见领袖的博客或帖子中包含广告，则必须在帖子上注明。

企业必须制定处理投诉的协议，以供潜在客户在购买前查看。在适当情况下，应说明合同期限及其终止条件。此外，出售数字内容的公司应确定相关的技术保护措施以及与其内容兼容的软件/硬件。

此外，该指令禁止使用自动将产品或服务添加到顾客购物车中的“预勾选框”（例如在购买机票时自动添加保险合同）。¹²

2. 明确和透明的条款

企业必须遵守有关合同确认的规则。¹³根据《消费者合同中的不公平条款指令》，合同条款应以简单易懂的语言表达。“不公平”一词通常被认为是为卖方（而非买方）创设的不正当优势。此类条款对消费者没有约束力。如果发现合同条款含糊不清，则应作出有利于客户的解释。

案例分析：匈牙利向苹果公司征收罚款

苹果公司在其 iPhone 上引入一项被称为 WiFi 助手的创新功能，以检测 iPhone 用户所使用 WiFi 信号的强度。如果 WiFi 助手检测到 WiFi 信号不够强，它会自动将 iPhone 切换到用户的移动网络，以便无缝连接到互联网。

用户可以关闭 WiFi 助手，但苹果公司并未提供有关此功能的具体信息（除一般条款和条件外），并且当 WiFi 助手将手机切换到移动网络时，用户不会收到通知。

负责执行匈牙利法律的匈牙利竞争管理局在实施《不公平商业行为指令》时发现苹果公司未向消费者提供重要信息，具体情形如下：(i) 未向消费者提供有关 WiFi 助手的充分信息（大多数消费者甚至不知晓该助手的存在），和 (ii) 未采用相应的解决方案以使消费者自行决定是否希望使用移动网络而非 WiFi 网络（例如接受或拒绝切换的文本通知）。

尽管转换到移动网络的费用不会为苹果带来收益，但当局认为这种做法也使苹果公司受益，因为消费者认为无缝连接是 iPhone 的产品功能。因此，当局对苹果公司征收超过 30 万欧元的罚款。

如果某一条款已与买方进行协商，则公司不承担责任。但是，如果它声称标准条款系经过协商，则由公司承担举证责任。

¹² 有关欧洲议会和理事会于 2011 年 10 月 25 日通过的有关消费者权利的第 2011/83/EU 号指令的 DG 司法指南文件，该指令修改欧洲议会和理事会第 93/13/EEC 号指令和第 1999/44/EC 号指令，并废除欧洲议会和理事会第 85/577/EEC 号指令和第 97/7/EC 号指令

¹³ https://europa.eu/youreurope/business/sell-abroad/on-line/index_en.htm#dop-consent-yes

3. 取消在线订单

根据《消费者权利指令》的规定，企业必须授予客户取消在线订单的权利。在交付订购商品后的 14 天内，客户有权终止与卖方达成的合同。在此期间内，客户必须通知卖方，卖方必须确认提款请求。这项权利使消费者有权在提交提款请求后的 14 天内获得全额退款（包括运费）。尽管如此，除非卖方同意承担或者未另行说明，否则客户承担退货费用。

除非客户另有约定，否则必须使用与初始购买时相同的付款方式进行退款。但是，在这种情况下，买方无需支付额外费用。此外，公司只需偿还与标准交付相关的费用，并且可以暂缓付款，直至收到退还的商品或者客户退货证明。

4. 交付、取消和赔偿

根据欧盟《消费者权利指令》¹⁴，公司必须在购买后 30 天内向其客户提供其订购的商品。如果消费者同意，可延长该期限。如果卖方仍未在最新期限内交货，则客户完全有权取消合同并获得赔偿。

如果交货日期具有重要意义（例如圣诞礼品），则公司必须授予消费者取消订单的权利，并且如果未在 30 天内交货则应向其进行赔偿。如果发生不当延误，卖方必须向客户进行赔偿。此外，企业应对运输期间发生的任何商品损坏或丢失承担责任，但客户与自己选定的承运人签订合同除外。

安全支付

数字经济为消费者提供由不同支付服务提供商提供的各种线上和线下支付选择方式，而不仅限于银行。就此而言，电子商务经营者必须确保其使用的支付系统达到最低水准的安全性和可靠性。

为了避免发生中断，并鉴于存在具有相同安全可靠水平的替代认证机制，并非所有交易都受到同等程度的保护（例如低价值支付）。但是，计划使用支付系统提供商的在线经营者应确保支付系统具备足够的安全水平。

2007 年通过的首个《支付服务指令》(PSD1) 的目的是确保整个欧盟的支付服务更为安全和更具创新性。由于后期的技术进步和在线支付选择的大量增加，2018 年初开始实施《支付服务指令 2》。该指令要求所有支付服务提供商（包括银行、支付机构或第三方提供商 (TPP)）必须证明其已采取适当的安全措施确保高水平的安全性。

支付服务提供商必须每年评估涉及的运营和安全风险以及任何缓释措施。为启动和处理电子支付而提出的最新且严格的安全要求能够降低欺诈风险并保护用户财务数据的机密性。

14 https://europa.eu/youreurope/business/sell-abroad/on-line/index_en.htm#dop-consent-yes

强客户认证 (SCA) 为消费者提供额外的安全保障。在发起支付时，强客户认证通过使用两种或两种以上要素来核证用户身份，其中包括信息（例如个人识别号码或密码）、持有物（例如卡片）和生物特征（例如指纹或语音识别）。这些要素是相互独立的，因此不符合某一项要素不会损害其他要素。

管理和解决纠纷

有效保护消费者权益还意味着实施公平、有效和透明的争议解决机制。一般而言，消费者有权在发生争议时选择诉讼地。这意味着消费者可以向其居住地法院起诉，也可以向电子商务经营者住所地所在国家的法院起诉。这可能导致多个国家的消费者向法院提起诉讼，并相应地导致电子商务经营者产生重大开支。

鉴于电子商务的全球性以及当事人所在的不同管辖区，重要的是企业应建立替代的庭外争议解决机制，以使消费者和经营者能够更快、更容易和更低成本地解决争议。根据适用法律，此类机制的使用不得阻止消费者向主管当局申请行政和司法命令。

广告

如今，博客和社交网络在促销方面如同过去的电视和广播一样有效。社交网站和博客的兴起带来一种将相关品牌推介给消费者的新方法。因此，在线广告部门经常面临法律挑战。

在这个快速决策和购买的时代，误导和虚假广告可能是需予解决的主要法律问题。照片修饰、误导性健康声明、低质量产品广告和隐形广告是最常见的投诉问题。

最后，同样重要的是互联网上的海量信息使得人们更加难以搞清误导和虚假广告。为了解决这个问题，许多网站正在制定对网站成员具有约束力的使用条款或其他文件。例如，Instagram 现在要求博客博主用特殊标签来标记促销帖子，未如此行事会被处以罚款。

随着广告业法规的迅速发展，参与者必须保持灵活，以遵守互联网最佳做法，并跟上不断变化的法律环境。

在线竞赛

社交媒体平台上的一些帖子邀请数字消费者“评选并中奖”，这些帖子被称为竞赛或彩票，受到法律和平台使用条款的约束。为确保他们的促销不构成非法彩票，营销人员必须遵守该等规定，包括强制披露赞助商信息的义务。

儿童广告

儿童属于受限制行为能力人，更容易受到广告的影响。因此，几乎所有国家的政府都对儿童敏感信息提出额外要求。例如，《通用数据保护条例》要求在收集 16 岁以下儿童的个人数据之前须征得父母的同意（但是，当地法律可能不同于该规则，将年龄限制降至 13 岁）。此外，应将所有在线广告进行分类并特殊标记。应特别注意不得向未成年人营销的产品——在这些情况下，广告商必须使用特殊标签以核实网站用户的年龄。以儿童为目标用户的广告不得直接促使儿童购买广告产品或者在实际上说服其父母或其他成年人为儿童购买广告产品。根据《不公平商业行为指令》的规定，此类广告构成不正当竞争。

直销

通过电邮、邮递员或按户送达等方式接触潜在客户的直销是最受约束的广告类型。遵守《通用数据保护条例》规定的义务给广告商带来沉重负担。例如，各组织需披露正在收集哪些数据以及在何地传输和存储数据；另外还需向用户提供退出方式。

从法律的角度讲，在进行直销时须取得用户“选择加入”许可的义务使得人们难以使用这种营销方式。此外，应将数据传输方式告知用户，其中包括在某些情况下作为营销活动主要来源的 cookie。根据知情同意原则，网站须披露数据收集的目的并将其告知用户，这意味着他们有权拒绝隐私和 cookie 政策。这些要求的范围可能排除一些特定广告活动。

元标记和搜索引擎

当客户在市场上搜索产品时，他们通常会使用 Google、Yahoo 和 Bing 等搜索引擎，这些搜索引擎会根据嵌入网站 HTML 代码中的元标记对每次搜索的结果进行排序。元标记用于描述网站，但有时包含其他内容（例如著名竞争对手的商标）以吸引流量。在这种情况下，元标记中的商标可能构成侵权，并可能导致法律诉讼。

用户生成内容

用户生成内容 (UGC) 可能会含有与内容相关的侵权。品牌在何时有权发布和使用有关其产品的博主照片？用户是否须对负面评论承担责任，如果“是”，在什么时候承担责任？社交媒体平台应当调整用户生成内容吗？根据网站平台规则和国家立法，这些问题的答案各有不同。

消费者保护措施不断发展

欧盟委员会的优先事项仍然是提高在线交易中的消费者保护。欧盟委员会已制定有关数字内容提供合同的指令。¹⁵《数字内容指令》的一项重大创新是向消费者授予与他们就数字内容交换个人数据之合同相关的权利。这与现行制度不同，现行制度只保护为获取该等内容进行付费的消费者。但是，如果企业未对个人数据进行商业性使用，则不适用该指令。

根据即将出台的指令，可给予两种形式的补救措施：

- “未提供内容的补救措施”：如果在首次购买时未提供数字内容，则允许进行第二次尝试，如果仍未提供，则消费者有权终止合同。
- “不符合标准的补救措施”：如果提供的内容不符合法律标准或者与消费者商定的标准，则消费者有权终止该安排、要求降低价格或者要求修理有缺陷的数字产品。

如果公司对其提供的内容进行重大修改，消费者还有权终止长期合同。¹⁶最后，与消费者签订的合同终止后，可要求数字内容提供商至少承担两年的责任。

若要发展在线业务，非常有必要遵守消费者保护法律。保持合规不仅可以避免遭到罚款或处罚，更重要的是可以保护客户关系和品牌。当在线评论能够达成或损害业务时，取得成功的关键是建立信任和尊重客户。

¹⁵ 第 8672/15 号文件

¹⁶ 欧盟理事会，布鲁塞尔，2017 年 6 月 1 日 (OR. en)，9901/17



识别数字消费者并与其签订合同

VICTOR NAUMOV AND GEORGY PCHELINTSEV, ST. PETERSBURG

在第四章中，我们重点关注最新的《通用数据保护条例》及其对数字消费者和整个电子商务行业的影响。在本章中，我们专注于电子认证的重要性以及电子合同的发展，这两者对于数字市场的平稳运行至关重要。

电子认证 - 法律要求

尽管客户的远程认证对于任何类型的电子商务都很重要，但是一些市场参与者受到与电子认证相关的特定法律要求的约束。特别是，大多数国家都要求金融机构（银行、资金转移机构和保险公司等）实施特定的客户尽职调查。除某些例外情况外，这些机构在与客户建立业务关系之前必须确定客户身份。

通过这些要求，国家立法者遵守金融行动特别工作组 (FATF)¹⁷倡导的国际标准以及欧盟通过的一般法律框架¹⁸。因此，在构建远程认证方案时，金融机构不仅要评估各个方案的商业有效性，还要评估是否符合适用法律的要求。

常用的电子认证方法

作为一般规则，客户尽职调查的级别取决于特定交易的风险等级。但是，根据常用方法，必须基于可靠和独立来源的文件、数据或信息来核实客户身份。

在这种情况下，大多数司法管辖区并不认为常用的电子认证机制（例如获取客户身份证件的扫描件）足以进行反洗钱尽职调查。在缺少可信任第三方的情况下，这种方法无法确保客户所提供数据的可靠性。因此，在实施之前必须仔细分析所有的远程认证方案。

统一的优势

欧盟已开始在单一市场内统一电子认证法规。特别是，欧盟委员会已制定有关电子认证的条例 (eIDAS)¹⁹，这为欧盟公共和信托服务电子认证的跨境承认创建法律框架。某一欧盟国家签发的电子身份证在其他所有欧盟国家亦须得到承认，只要它们符合法规要求并已向欧盟委员会报告。

此外，本文件为合格和不合格的信托服务规定同一法律框架，包括电子签名、电子印章或电子时间戳的创建、验证和确认以及与这些服务相关的证书。因此，有关电子认证的条例框架是欧洲单一市场的基石之一，它涵盖电子认证和验证的所有要素。

欧盟委员会特别关注金融科技的发展趋势以及银行在将来以数字方式认证客户的能力。同时，欧盟委员会希望确保现代远程认证工具的安全，其不会给消费者或系统带来新风险，同时符合欧盟数据保护法。

为了确定远程认证方法符合这些要求，欧盟委员会于 2017 年底成立电子认证和远程“了解您的客户”流程专家组。²⁰该小组的任务是探讨与远程认证方案的使用问题以及是否根据有关电子认证的条例向它们发送通知。该小组还在探讨符合反洗钱规则的其他创新数字流程。在适当情况下，该小组将协助欧盟委员会编写与数字认证相关的指南。

17 FATF (2012-2017)，《打击洗钱、恐怖融资与扩散融资的国际标准》，FATF，法国巴黎。

18 欧洲议会和理事会于 2015 年 5 月 20 日通过的有关防止利用金融系统洗钱和恐怖融资的第 2015/849 号指令，修改欧洲议会和理事会通过的第 648/2012 号条例，并废除欧洲议会和理事会通过的第 2005/60/EC 号指令和第 2006/70/EC 号指令，OJ L 141, 5.6.2015, 73 117 页。

19 欧洲议会和理事会于 2014 年 7 月 23 日通过的有关内部市场电子交易的电子认证和信托服务的第 910/2014 号条例，并废除第 1999/93/EC 号指令，OJ L 257, 28.8.2014, 73 114 页。

20 European Commission Decision of 14.12.2017 setting up the Commission expert group on electronic identification and remote Know- Your-Customer processes.

电子合同的发展

在当今数字驱动的世界里推动和管理业务时，电子合同的概念至关重要。尽管在 20 世纪 80 年代即已出现电子合同，但是电子商务从 20 世纪 90 年代初才开始广泛增长。为应对这种快速增长，欧盟于 2000 年通过《电子商务指令》，以制定规范该行业的法律框架。该指令的目的是统一和澄清适用于整个欧盟互联网业务的规则，并保护消费者利益。

在更先进、复杂和广泛的信息技术的驱动下，当前的数字化转型代表市场参与者和监管者面临的最新法律挑战。因此，欧盟正审议两项特殊立法提案：关于商品在线和远程销售合同的指令以及关于提供数字内容合同的指令。这两项指令的审议工作目前都已接近完成。

解决重要事宜的法律

从历史上看，与电子合同相关的待解决重要事宜包括：确定联系人、证明就某些条款达成一致，以及核证电子签名或其他同意形式。随着商业和法院实践的发展，这些事宜已得到解决。

为了统一该领域的规则，欧盟最近通过《有关认证和信托服务指令》，该指令已于 2016 年 7 月生效。该指令规定三种类型的电子签名：基本、高级和合格的电子签名以及法律实体的电子印章。

适用法律

互联网业务固有的另一个主要法律问题是确定适用于特定交易和司法管辖区的法律。尽管由于各成员国之间的立法统一，这个问题在欧盟内部可能不如世界其他

地区那么严重，但是各成员国法律之间仍存在差异，其他国家的法律之间更是缺乏统一性。

针对这个问题，电子商务不仅要特别注意其网站的内容或者销售和服务条款，还要特别注意其宣传业务和设定合同架构的方式。

电子合同不仅与传统业务中的合同不同，它可能是只以数字形式存在的产品或服务合同，或者存在于区块链中并且无需任何人为干预即可执行和完成的合同。另外还出现全新的互动形式，例如 Machine2Machine 或 Machine2Business。

资产和负债令牌化的最新趋势创造出巨大的机会，从而能够以数字形式销售几乎任何物品。但是，自动创建和完成数字合同须实施更复杂且即时的文档处理，其中涉及使用智能手机等设备来采取先进的认证和签名方法。

此外，合同的自动化带来网络安全问题，并对合同解释和无效性等带来新的课题。

下一代挑战和趋势

随着数字化转型时代的到来，传统电子商务合同法再次面临挑战。软件即服务 (SaaS)、物联网、大数据、云端、人工智能、区块链和增强现实等技术正在改变商业和法律实践，并要求就各种问题制定和调整法规。



A person is holding a tablet that displays a fashion website. The website features a large image of a red dress and the text "THE NEWEST TRENDS". Below this, there is a section titled "WHAT'S NEW" with a grid of clothing items. One item is labeled "BRILLIANT BLUE £180". The background is a blurred image of a person's hair and shoulders.

电子商务、金融科技的发展以及加密货币的增长

MATTHIAS EGGERT, 慕尼黑; NATALIA SELyakOVA, 基辅

在前述章节中，我们探讨数字市场的增长以及这种快速增长在规范电子商务和保护数字消费者方面所面临的挑战。在本章中我们关注金融服务部门的技术发展，以及政府在解决关键细分市场中数字化发展和加密货币创新方面所面临的法律挑战。

什么是金融科技？

金融科技是指实现最新金融服务或者促进现有金融服务的技术解决方案。金融科技处于严格监管的金融服务和数字创新的交叉口，它使得新产品和新业务模式进入市场。市场参与者既包括新设公司也包括传统和成熟的市场领导者。

新设公司可采用电子平台等方式提供技术解决方案或中介功能，它们也可只提供融资。移动应用程序、数据分析、人工智能、云计算和分布式分类帐技术——所有这些新技术为金融科技解决方案创造机会。

金融科技部门的核心包括支付服务、融资服务、投资服务以及咨询和中介服务。每一部分均为数字消费者提供各种不断发展的选择方案。

发展与增长

在过去几年间，有关最新金融科技的创业活动一直表现强劲。尽管一些市场评论员指出商业模式已开始从B2C转向B2B，但是其他报告称呈现平均分布。在过去十年间，金融科技在欧洲的投资和并购活动保持强劲势头，其中2014年和2015年是高峰期，2016年处于低谷。市场报告显示，成熟公司越来越多地参与并购活动。

根据该行业的投资和并购报告，到目前为止，欧洲金融科技的主要中心一直是伦敦，而法国和德国正迎头赶上。许多欧洲国家已设立孵化中心以促进金融科技新设公司的发展，并促进金融科技与传统市场参与者之间的合作。在英国和法国，这些活动集中在伦敦和巴黎，在德国的许多城市也已设立金融科技中心，其中包括柏林、慕尼黑、法兰克福、汉堡、斯图加特和科隆。

未来的增长和监管

在最近十年间的大部分时间里，欧洲机构一直在关注金融科技行业的各个方面。例如，欧盟委员会一直在审查众筹领域，并于2016年5月发布一份报告。欧洲银行管理局(EBA)、欧洲证券和市场管理局(ESMA)以及欧洲保险和职业养老金管理局(EIOPA)一直在审查金融咨询自动化的发展，并于2016年发布一份报告。

欧洲证券和市场管理局针对应用于证券市场的分布式分类帐技术的风险和收益进行分析，并于2017年2月发布一份报告。

最近，欧洲机构正采取更全面的方法。

2016年11月，欧盟委员会成立金融科技内部工作组，就金融科技的作用进行公众咨询。欧盟委员会于2017年发布回复摘要。欧盟委员会还于2017年3月发布消费者金融服务行动计划。

欧洲银行管理局也于 2017 年对欧盟现有的金融科技企业及其活动和商业模式进行调查。在欧洲银行管理局于 2017 年 8 月发布的讨论文件中列明调查结果，其中称：“由于金融科技适应市场发展，并可能导致风险偏好的修正，因此其目前的增长也可能改变监管机构的范围和目标。欧盟及其他地方的公共机构已开始调查金融科技对金融体系及其监管和监督事宜的影响，这一点并不令人意外。”

金融科技在欧洲的发展情况如何？

迄今为止，由于金融科技行业的发展，欧洲已制定《支付服务指令》(PSD) 和《支付服务指令 2》(PSD2)。此外，欧洲机构看起来仍处于事实调查阶段。现阶段，似乎很可能对现行法律进行修订。

但是，目前尚不清楚是否会制定全新的法律。在欧洲可能就分布式分类帐技术制定新法律。在欧洲银行管理局于 2017 年 8 月发布的讨论文件中出现另一个可能进入欧洲立法安排的概念，即监管“沙箱”，它能够在相关当局的支持下并在有限期间内验证和测试商业模式。

对欧洲企业和数字消费者的意义

除《支付服务指令》和《支付服务指令 2》以外，在欧洲运营的金融科技企业需遵守普遍适用的法律法规，但是现阶段特定金融科技法规很少。相关企业特别需考虑以下事宜及其对企业和消费者的影响：

许可

金融科技企业需要在早期阶段确定他们的商业模式是否须取得许可证。金融科技企业采取的许多商业模式须取得许可证。在许多（并非所有）欧盟成员国中，如果经营某些业务的企业未取得许可证，会被处以行政罚款。这种情形甚至可能构成刑事犯罪，可能被处以监禁和/或禁止担任提供银行或金融服务之公司的董事。

举例来说，在欧盟成员国从事以下（并非所有）活动须取得许可证：

- B2C 贷款
- B2B 贷款
- 保理
- 反向保理
- 贷款经纪人
- 向公众吸收存款
- 金融工具经纪
- 资产管理
- 付款服务
- 收款服务

在确定是否须取得许可证时，金融科技企业应考虑潜在交易各方所在管辖区内的规则。例如，在从事贷款业务时，需考虑借贷双方的管辖地。在从事保理业务时，应主要考虑应收账款的卖方及相关买方的管辖地。此外，债务人所在地也可能具有关联性。

有时获得低额许可证豁免。但是，不应假设拟进行少量交易或者拟交易的价值较低，从而可自动获得豁免。例如，就贷款而言，发放首笔贷款时视情况可能须取得银行牌照。

如果须取得许可证，该要求通常包括以下内容：

- **组织形式和最低出资金额：**某些银行和金融服务只能由按某种法律形式成立的实体提供，并且最低法定资本可能高于普遍适用的公司法中就相关组织形式规定的金额。
- **可靠性证据：**只有当相关实体的管理层包括一名或多名能够在相关领域展示出全面专业经验的人员时，方可提供某些银行和金融服务。
- **商业计划：**作为取得许可证的先决条件，许多银行和金融服务须制定可持续的商业计划。
- **监管资本：**基于相关业务的数量，只有当存在监管权益资本时方可提供诸多银行和金融服务（这与上述最低法定资本的要求无关）。

最近，越来越多的金融科技企业开始设法为自身配备足够的工具和人力资源，以获得所需的许可证。例如，据报道，一些金融科技企业已在英国和德国获得完整的银行许可证。金融科技企业也可采取以下一种或两种策略。首先，他们可以修改活动范围，从而无须取得许可证。另外，他们可以与已取得许可证的合作伙伴进行合作，以从事该合作伙伴可从事的活动。

募资

在进行公众募资时可能须取得许可证和/或符合注册要求。此外，可能还须编写招股说明书。但是，对于种子和早期阶段的出资，可提供低额豁免。

保护数字消费者

如第四章所述，《通用数据保护条例》于 2018 年 5 月 25 日生效。采取 B2C 模式的金融科技企业通常需遵守《通用数据保护条例》，而采取 B2B 模式的金融科技企业只有在其服务的对象包括自然人时方须遵守该条例。

不遵守《通用数据保护条例》规定的要求可能被处以行政罚款，金额可高达全球年营业额的 4%。为了进一步增强《通用数据保护条例》的实施，欧盟成员国的法律可规定额外处罚。

结语

当随着时间的推移对这些新技术解决方案进行测试时，它们本身可能成为（在某些情况下甚至取代）传统的被监管金融服务。与此同时，金融部门实施数字化转型和创新的强劲趋势带来一系列新的法律风险，须予评估和解决。

焦点问题: 加密货币的发展

随着金融科技创新的不断发展和演变, 它们将继续改变公司的面貌。区块链是一项重要也是最常讨论的金融科技创新。区块链使用分布式分类帐技术, 这是一种去中心技术, 可使企业和数字消费者快速有效地处理合同和交易, 从而消除对中介机构的需求。

自 2009 年开始出现加密货币以来, 利用颠覆性区块链技术, 世界上最广为人知和最广泛使用的加密货币就是比特币。之所以推动比特币等加密货币的增长, 是希望能够提高效率和消除不必要的成本, 同时拥有一种可以在各种市场中易于使用的货币。许多领先的金融机构已表现出对试用区块链技术的兴趣和意愿。事实上, 有些机构正开发自己的加密货币, 例如花旗银行 (Citicoins); 瑞银、德意志银行、桑坦德银行和纽约梅隆银行 (多功能结算币); 高盛 (SETLcoin); 英格兰银行 (RsCoin); 和中国人民银行 (RMBCoin)。

尽管在某种程度上由于加密货币的去中心化和匿名性, 加密货币的吸引力持续增长, 但是它们尚未被任何国家政府认可为首选货币模式。

不过, 许多国家一直非常关注对加密货币进行监管, 特别是越来越多的主流公司在各种行业中探索加密货币和区块链技术的优势。欧洲央行行长马里奥·德拉吉最近表示, 欧洲央行无权监管加密货币, 但我们发现一些欧洲国家正考虑实施监管。

在德国, 相关的监管机构是德国联邦金融监管局 (BaFin)。德国联邦金融监管局通常允许将比特币和其他加密货币以会计单位的形式作为金融工具使用。德国财政部考虑将加密货币视为无形资产, 它们通常须缴纳所得税和增值税, 具体取决于首次代币发行和加密货币的特定设计。

尽管联邦金融监管局的官方立场是中立的, 但在 2017 年 4 月, 它禁止 Onecoin (迪拜) 和 OneLife Network (伯利兹) 在互联网上提供公开访问系统以使用 OneCoins 进行交易。联邦金融监管局予以禁止的理由是其认为 OneCoin 业务属于《德国银行法》(KWG) 的自营交易, 根据该法第 32 条的规定须取得许可证。





在数字环境中行使知识产权

STEFAN DITTMER 博士, 柏林; CONSTANTIN REHAAG 博士, 法兰克福;
和 HANNA KAROLINE HEIDKAMP, 法兰克福

如第二章所述，知识产权是任何数字化转型项目的关键问题。知识产权允许创作者从其科学、技术、文学或艺术作品中受益，并使所有者从其对创造活动的投资中获益。知识产权法起着非常重要的作用，它不仅保护公司专有技术免遭滥用，还促进社会的原创、创造和创新活动。

虽然先进和颠覆性技术为创新提供令人振奋的可能性，但是具有讽刺意味的是，它们也助长了侵犯知识产权的行为。在共享经济中，通常很难保护内容不被共享或者难以证明侵权何时发生。

在当今的数字环境中，对知识产权的认识以及如何保护和商业化这些知识产权已变得至关重要。因此，任何数字化转型项目都需考虑如何保护自身的知识产权，同时确保不侵犯他人权利。

知识产权类型

在规划数字化转型时，需牢记世界知识产权组织定义的五种知识产权：

版权和相关权利：版权法允许作者、艺术家和其他创作者保护他们的文学和艺术创作，特别是表达形式。

专利：专利是指专利局为发明授予的专有权，所谓发明是指就产品或程序提供最新处理方式，或者提供某一问题的最新技术解决方案。它在有限期间（通常为 20 年）内为权利人提供发明保护。

商标：商标是指识别个人或公司生产或提供的某些商品或服务的独特标志。它可以是单词、字母和数字中的一项或多项组合。它也可以包括图画、符号或三维标志，例如商品的形状和包装。

工业设计：工业设计是指物品的装饰或美观形式，并应用于各种工业品和手工艺品（包括时尚物品）。

地理标志：地理标志是指针对来自特定地区并由此具备相应品质或声誉的商品所使用的标志。通常来说，地理标志包括商品原产地名称。它广泛应用于农产品，但也可用于保护因特定的当地技能和传统而产生的独特产品。

尽管世界知识产权组织并未提及商业秘密，但是它们在创新以及数字和数据经济中发挥着越来越重要的作用。针对不受版权保护的数据库中的部分数据，如果没有保护该等数据所有权的特定权利，则商业秘密保护通常成为保留和商业化数据价值的唯一途径。

商业秘密的重要应用领域是加密技术

数字世界中面临何种知识产权挑战？

如上所述，技术进步也可助长盗版、假冒和其他知识产权侵权行为。与此同时，就数字消费者而言，我们看到用户创建在线内容、整合和接触数字文化的现象。那么，我们如何才能做好最充分的准备，从知识产权的角度应对数字化转型的挑战？

首先让我们探讨盗版的挑战和颠覆性技术的出现。如果在未经权利人授权的情况下制造、销售或分发受保护物品，则构成知识产权侵权行为。除可测定的损失外，从长远来看，侵犯知识产权对经济的影响更为严重。侵犯知识产权会产生不利的社会和经济影响，例如失业和降低创造和创新动力。

在数字时代，盗版和假冒问题尤为重要。未经授权的数据共享、集成、利用和公开披露是最受关注的领域。技术的不断发展和互联网的全球扩张使得人们更容易获得有关产品的信息，其中包括高科技产品，例如药品、计算机芯片和软件等。

而且，3D 打印等新制造技术使生产盗版商品变得前所未有的简单。最近出现的这些新趋势仍与“传统”的假冒和盗版产品行为具有关联性，据欧洲刑警组织称，这些最新假冒和盗版产品金额占欧盟进口总额的 5%（即 850 亿欧元）。

互联网的匿名和无边界特征为知识产权侵权创造理想的环境。对于暗网来说尤其如此，暗网是指一种可通过特殊软件或通信协议访问的网络，它已成为地下活动的温床。令人担忧的是，跨境犯罪集团越来越多地实施侵权行为，这些集团利用互联网进行组织、分销、客户服务和在线支付，从而使权利人难以通过将侵权人诉诸法院和向其提起民事诉讼来行使其权利。

在贸易变得越来越国际化并且为了促进贸易流动通过区域经济一体化来消除边界的同时，打击盗版和假冒的努力却相对落后。

数字环境还对知识产权执法提出立法挑战，这些挑战尚未在任何全球协议中得到解决。针对通过互联网实施的侵权行为，在有效执法方面存在非常明显的障碍，例如侵权人身份、服务提供者责任、知识产权行使、在国外受保护在线权利的处理以及法院管辖权问题。

我们如何保护知识产权？

无论是政府、企业、消费者，还是只在国家层面行事的一方，都无法单独赢得打击侵犯知识产权的斗争。在全球化商业环境中，国际合作是保护知识产权的关键，官方机构在打击盗版和假冒行为方面发挥着至关重要的作用，包括欧洲刑警组织、世界知识产权组织和打击假冒和盗版商业行动工作组 (BASCAP)。除这些官方机构以外，许多知识产权权利人也正进入在线市场[侵权人可能（无意地）利用在线市场销售盗版商品]，以了解侵犯知识产权的情况并寻求合作以打击知识产权犯罪。许多公司正在制定安全策略，以采用一系列技术和功能来打击侵犯知识产权的行为：

- 水印：水印的最大优势是有可能阻止在未经授权的情况下使用相关内容。水印是添加到内容中的一条信息，用于确定单个内容的特征和所有权。
- 指纹识别：数字指纹是指由 1 和 0 组成并用于标识内容的独特模式。
- 数字版权管理 (DRM) 技术：数字版权管理技术通过识别内容、控制访问、保护作品完整性以及确保访问付款来保护版权。保护数字内容的另一种方法是实施技术保护措施 (TPM)。

访问数字内容

尽管面临知识产权挑战，但是数字化颠覆在线提供越来越多的数字文化和用户创建内容，其也会产生积极影响。

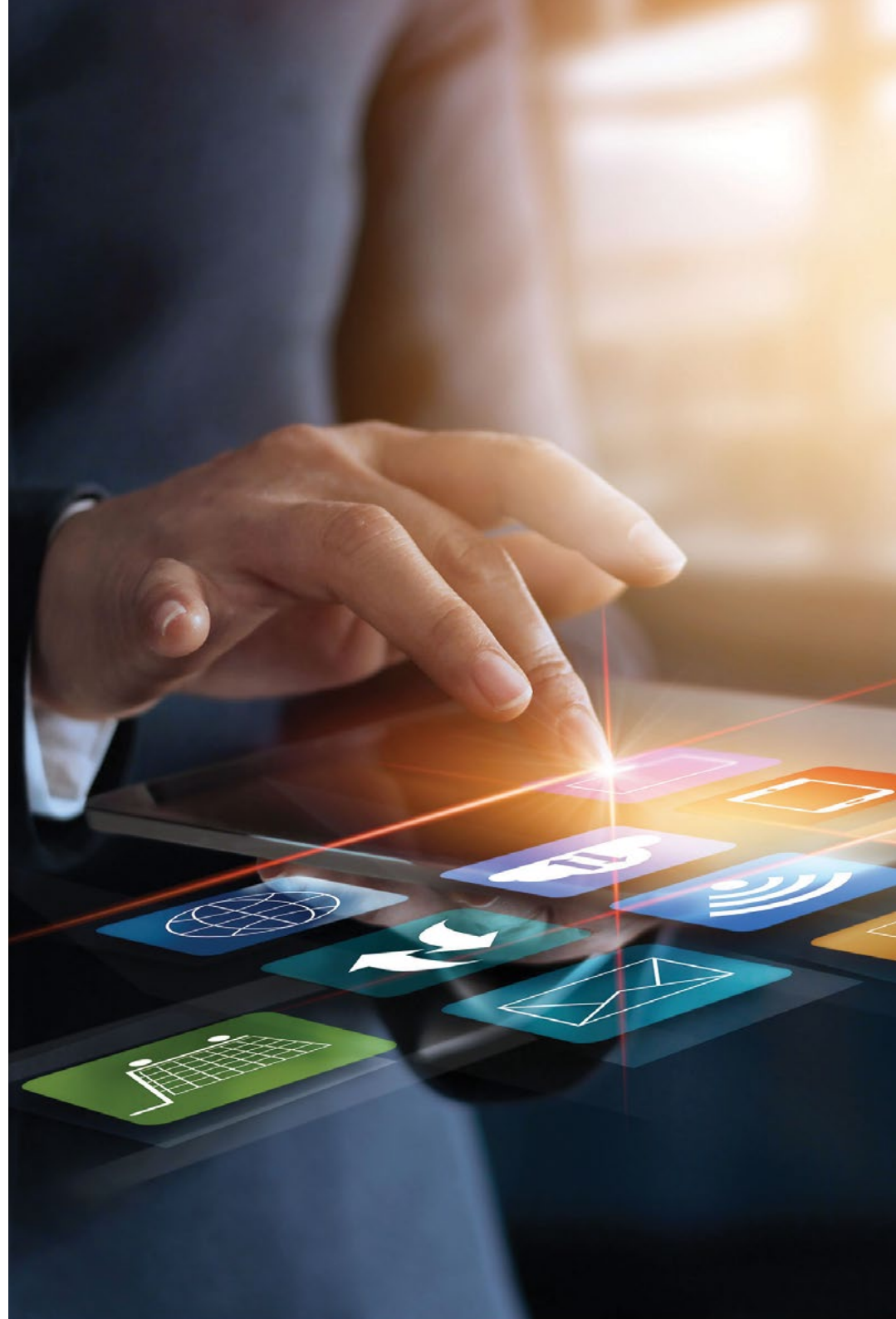
欧盟委员会最近宣布采取措施，在奖励创造者投资和促进尽可能广泛获得受知识产权保护的商品和服务之间取得更好的平衡。

例如，针对版权人不明或者无法确定版权人地点以获得版权许可的无主作品，欧盟委员会正引入立法以允许该等作品的数字化和在线可用性。欧盟委员会还在寻求简化欧盟版权的集体管理，并创建欧洲版权准则和“统一”版权。欧盟还在持续努力减少通过互联网销售假冒商品的现象。

发展方向

在当今的数字世界中，大量的分销商品机会带来不断增加的最新挑战。国际知识产权法律框架为传统产品和数字内容的所有者提供一致和灵活保护。但是，无论是法律框架还是监管干预，都无法跟上技术发展速度以及寻求绕过该等技术的盗版侵权人。

在规划数字化转型时，重要的是要牢记对于鼓励创新和保持创造的多样性而言，知识产权保护至关重要，并应将该等保护措施纳入战略中。但是，由于保护知识产权的理念在共享经济中受到冲击，政策制定者和行业参与者也应考虑以阻止侵权行为的方式为创造者提供报酬的创新方法。





大数据和欧盟竞争法

JAMES VENIT, 布鲁塞尔

在启动数字化转型项目之前，了解欧盟在大数据、数字网络和数字平台上应用反垄断规则的情况非常重要。迄今为止，欧盟委员会主要在两个合并案件中处理大数据问题——Facebook/WhatsApp（2014 年）和微软/领英（2016 年）。在这两个案件中，尽管有各种说法，但是欧盟委员会并未介入。

与此同时，德国和法国在确定适用于数字平台和网络的分析框架（包括数据与市场力量之间可能存在的关联）方面实际上比欧盟委员会更为活跃。法国竞争管理局已提起两个相当传统并涉及数据（但非大数据）的案件，德国联邦卡特尔局提起一个相对新型案件，其中声称 Facebook 可能滥用其主导地位而未遵守德国数据保护法律。

欧盟合并案件

Facebook/WhatsApp

欧盟委员会对三个市场进行审查：(i) 消费者通信服务；(ii) 社交网络服务；(iii) 在线广告服务。消费者通信服务存在横向重叠，合并后实体在其中将拥有 30-40% 的份额。

欧盟委员会确定一些减轻 Facebook/WhatsApp 合并所带来任何负面网络影响的因素，其中包括 (i) 消费者通信是一个快速发展的产业，其中的转换成本和进入门槛都很低；(ii) 多链路的普遍性；即单个客户使用多个通信应用程序；(iii) 由于各方未控制网络或任何移动操作系统的任何核心部分，因此并不存在客户锁定；和 (iv) 由于 Facebook Messenger 和 WhatsApp 均未在大量手机上进行预装，因此不存在任何现状偏差。

欧盟委员会的结论是，由于 WhatsApp 和 Facebook 之间的整合存在技术上的困难（例如难以匹配用户名称以及跨平台通信方面的工程障碍），合并不太可能加强网络效应。即使 WhatsApp 和 Facebook 实施一些整合，也可通过两个网络之间已存在的显著重叠来缓解这种情况。

欧盟委员会还审查 WhatsApp 作为具有广告价值之用户数据的潜在来源以及通过合并增强 Facebook 在线广告地位的可能性。审查结论认为，除隐私问题以及客户可能转向侵入性较低通信应用程序的风险以外，当合并后在谷歌、苹果、亚马逊、eBay、微软、AOL、雅虎、Twitter、领英、Adobe 和 Yelp 等竞争对手之间仍存在足够的在线广告服务竞争，即使合并实体开始收集和使用 WhatsApp 用户数据。在整个网络上收集的数据中，Facebook 和 WhatsApp 总共只约占 7.5%，谷歌占 33%，其他所有各方约占 69%。

尽管该合并使电信公司失去即时通讯的收入，因此遭到电信公司的强烈反对，但是市场调查并不支持电信公司的损害主张。

2017 年 5 月，因 Facebook 在合并调查期间提供误导性信息，欧盟委员会向其处以 1.1 亿欧元的罚款。Facebook 告知欧盟委员会其无法与 WhatsApp 的用户账户建立可靠的自动数据匹配，但是在 2016 年 8 月，WhatsApp 宣布可能将其用户电话号码与 Facebook 用户身份相关联。在德国，汉堡数据保护局称其会阻止 WhatsApp 将其用户数据传输给 Facebook。在第二个案件中，欧盟委员会只关注程序性问题（提供误导性信息），并且其对 Facebook 提供误导性信息作出的罚款决定确实影响到就消费者通信服务市场不存在不利影响的结论。

微软/领英

在微软/领英案件中，欧盟委员会的审查工作重点关注三个市场：

(i) 专业社交网络服务；(ii) 客户关系管理软件解决方案；和 (iii) 在线广告服务。

鉴于重叠程度有限以及各方的合并份额低于 10%，欧盟委员会对于在线非搜索广告服务的横向重叠没有任何担心。

欧盟委员会不担心数据库组合（包括工作、职业经历、专业联系、电子邮件或其他联系人、搜索行为等），但确实发现两个潜在的反垄断问题：(i) 为了向广告商提供这些数据而创建或加强市场力量；和 (ii) 为了向广告商提供数据而构成影响竞争对手的进入/扩张壁垒，这些竞争对手需要该等数据才能在市场上展开竞争。

欧盟委员会注意到，各方之间的任何数据共享可能受到数据保护规则的限制或者被该等规则阻止。欧盟委员会还指出，除有限的例外情况，微软和领英不会出于广告目的向第三方提供数据，并且他们的数据库组合不会构成进入壁垒，原因是在微软控制范围以外就广告目的存在大量的有价值互联网用户数据。

关于潜在的纵向问题，欧盟委员会要求微软承诺：

- 确保 PC 制造商和分销商可自由地不在 Windows 上预装领英，用户可自由地删除预装的领英
- 具有竞争关系的专业社交网络服务提供商可与微软办公套件维持在当前的互操作水平
- 具有竞争关系的专业社交网络服务提供商可访问 Microsoft Graph，它可用于构建访问存储在微软云端的个人数据和电子邮件的应用程序和服务

这些承诺是指与大数据问题无关的标准纵向承诺，欧盟委员会并不担心微软收购领英的数据库。

国家层面的活动

与欧盟委员会相比，国家竞争管理机构在大数据以及数字网络 and 平台方面的活动要活跃得多。

关于数字平台和网络的法德联合文件

2016 年 5 月，德国联邦卡特尔局（“FCO”）和法国竞争管理局（“AdC”）发布一份关于数字平台和网络的联合文件。²¹该文件提供有关数字平台和网络竞争问题的路线图，并确定以下可能产生的反垄断损害：

- 作为市场力量来源的数据
- 市场透明度提高对价格产生的潜在影响

- 与数据相关的反竞争行为，包括拒绝访问；歧视性访问；独家经营、捆绑、杠杆以及价格歧视

有关评估数字平台和网络市场力量的联邦卡特尔局报告

2016 年 6 月，德国联邦卡特尔局发布一份有关评估数字平台和网络市场力量的报告。该报告就大数据指出，在评估数字平台和网络的市场力量时，需分析数据源的访问，但是数据控制本身并不代表市场力量。相反，需逐项评估收集数据的基础、它们的竞争相关性、是否可以复制以及组合不同来源数据的选项。联邦卡特尔局报告中确定可能产生或降低市场力量风险的以下积极和消极因素。

表明市场力量的正面因素	表明缺乏市场力量的负面因素
(i) 可产生相对优势的强大自我强化反馈环路 (ii) 匹配平台具有强大的双向、正向和间接的网络效应 (iii) 如果一个平台明显优于竞争对手平台，强大的网络效应是其占据主导地位的首要指征 (iv) 构成进入壁垒的直接和间接网络效应 (v) 规模经济，这既可以构成进入壁垒，也可以加强平台固有、自我强化的正反馈环路	(i) 多链路 (ii) 平台差异化 (iii) 平台拥堵²²

21 如果互联网企业提供允许通过间接网络效应连接的两个或更多用户组之间直接交互的中介服务，则将其视为平台。如果互联网企业提供允许相同组的用户之间进行交互从而产生直接网络效应的中介服务，则将其视为网络。当然，一些商业模式同时具备平台和网络要素：社交网络 (Facebook) 是提供平台的受众，并通过广告获利。

22 拥堵是指平台的技术/物理限制，这可能导致无法接纳更多用户。虚拟拥堵是指如果平台的用户组规模变得过于庞大，平台的效用就会下降。

该报告指出，具有高水平直接或间接网络效应的平台/网络市场往往高度集中，但由于网络效应对竞争的影响，市场份额在评估市场力量方面的关联性可能不大。但是，基于用户群的高水平市场份额可能与间接网络效应导致的相对优势风险具有关联性。

该报告促使联邦卡特尔局寻求修订德国竞争法，以使其有能力对数字平台和网络采取执法行动。这些修正案将：

- (i) 允许针对搜索引擎或价格比较网站等数字服务界定相关反垄断市场，尽管其中不存在金钱交易；
- (ii) 通过网络效应、规模效率、数据访问和创新等因素，提供额外工具来评估双向数字平台的市场力量；
- (iii) 扩大德国的合并审查范围，从而涵盖交易价值超过 3.5 亿欧元的合并交易，即使目标企业的营业额低于 500 万欧元。

竞争管理局提起的案件

法国竞争管理机构参与两个案件，并要求相关公司向竞争对手提供数据库。

GDE/Suez

在这个案件中，竞争管理局采取临时措施，要求 GDF-Suez 编制其在垄断法国能源市场时从客户处获得的消费数据，从而供竞争对手利用以便于它们进入市场。

Cegedim

竞争管理局要求法国领先的医疗信息数据库提供商将其主数据库出售给在相邻市场中为客户关系管理而使用竞争对手软件的客户。Cedegim 涉及一个典型的捆绑案例——Cegedim 已将其数据库的访问捆绑到其客户关系管理软件的使用。

英国竞争和市场管理局（“CMA”）

Trod/GB eye - 使用价格算法实施横向价格固定在 Trod/GEb eye 案件中，两家公司使用自动再定价软件来实施其达成的协议，以使亚马逊的英国网站上双方的价格保持一致。除了就横向价格固定事宜对两家公司进行处罚外，竞争和市场管理局还警告软件供应商，称如果它们协助客户使用软件来实施非法的价格垄断协议，则可能违反英国竞争法。²³

由于使用定价算法的现象变得更为突出，对其进行监管的问题越来越引起关注。竞争和市场管理局局长 David Currie 怀疑监管机构是否拥有相应的工具以跟上不靠人为介入进行学习的价格算法，Vestager 专员表示，如果卡特尔组织通过价格算法来实施价格固定协议，可能被处以更高金额的罚款。

就 Vestager 专员的警告和 Trod 案件而言，其中涉及当事人达成固定价格的协议并使用算法来实施该非法协议。传统竞争法就处理侵权行为的所有必要工具作出规定。而 Currie 先生担心的是不同的情形，这涉及使用人工智能来协调价格，其中没有任何协议或者人为参与。鉴于缺少人为介入，竞争法可能无法处理这种情形，尽管法规禁止使用该等算法。

23 欧盟委员会在最近涉及华硕的最低转售价格 (RPM) 调查中似乎表明，算法的使用向纵向最低转售价格中增加横向因素。定价软件能够统一最高价格，从而在横向维度上实施最低转售价格

联邦卡特尔局提起的案件

在所有国家当局中，德国联邦卡特尔局最为积极地处理数据问题。

联邦卡特尔局向 Facebook 提起滥用案件

2016 年，联邦卡特尔局提起一起案件，指控 Facebook 违反德国数据保护法的行为构成滥用支配地位。联邦卡特尔局称 Facebook 未向会员充分披露如何使用数据和/或保护其数据隐私，这构成剥削性滥用行为。目前还不清楚联邦卡特尔局的方法是否涉及任何反垄断损害理论。如果数字平台基于向用户提供的条款展开竞争，隐私保护可能构成竞争性要素。在这种情况下，如果占主导地位的公司提供这种保护的壓力较小，那么未如此行事可能表明存在市场力量。

目前不太清楚的是，不遵守数据保护法是否构成违反竞争法。将其纳入竞争范畴可能是执行数据保护法的有效方式，但是很难确定相关行为如何构成反垄断违规行为，特别是在市场力量与不遵守隐私法律之间没有任何因果关系的情况下。

联邦卡特尔局在 Facebook 案件中的做法与欧盟委员会的做法很不相同，欧盟委员会在 2006 年采取的立场是个人数据相关问题不属于竞争法的范畴。欧盟委员会在 Facebook/WhatsApp 案件中重申这一观点，当时它表示“由于...任何隐私相关问题都源于数据集中度的提高...[合并]不属于欧盟竞争法规则的范围，而属于欧盟数据保护规则的范围。”

联邦卡特尔局对亚马逊的调查

最近，联邦卡特尔局表示出对于亚马逊作为零售商和营销平台双重角色的担心。联邦卡特尔局主要担心的是亚马逊同时作为平台和零售商的角色，可通过访问竞争对手数据获得竞争优势。尽管以数字形式呈现，但是联邦卡特尔局确定的问题可能不会超越同一商家在上下游市场展开运营或者分销其自身和竞争对手的产品时产生的更为传统的反垄断问题。

结语

如先前调查表明，欧盟委员会迄今尚未发现任何合并案件中涉及大数据竞争问题，在这两个案件中，它考虑的是数据库组合事宜。尽管德国和法国竞争机构都编制研究报告，其中列明与大数据以及数字网络 and 平台相关的分析性反垄断路线图，但是受调查各成员国的案件都未解决大数据问题。

尽管在这里关注的是由于使用人工智能进行定价而缺少共谋特征的普通卡特尔活动，但是在国家（英国）和欧盟委员会层面上对使用算法来促进卡特尔活动的认识和关注度也有所提高。

数字经济和旧经济之间的冲突以及大数据的吸引力不太可能消失。因此，更主要的问题可能是在将来何时发生涉及大数据或者数字平台和网络的案件。

A photograph of four business professionals in a modern office setting, standing near large windows that offer a view of a city. The scene is bathed in warm, golden light, suggesting late afternoon or early morning. The individuals are engaged in a conversation, with one man gesturing towards the others. The image has a teal-colored overlay at the bottom, where the title and author information are placed.

数字化转型对雇员的影响

FRANK LENZEN, 法兰克福

尽管本指南主要关注数字客户，但是数字化转型战略中必须考虑的另一个首要问题是关键的利益相关方群体——雇员。在当今的知识经济中，雇员是许多公司最宝贵的资源之一。此外，雇员处于为客户提供积极体验的第一线。因此，值得关注的是数字化转型中的一些劳动法事宜。

如今，技术进步彻底改变人们如何看待工作。通过技术，我们的工作地点和时间获得更大的灵活性。我们的关系变得更加紧密，可以与世界各地的同事进行远程协作。我们可以在家里、机场或喜欢的咖啡馆工作。在线工作平台现已产生“零工经济”，人们在该等平台上可独立工作，并逐个项目地参与其中。

尽管大多数雇员都乐于更为灵活地工作，但也存在需予解决的潜在重大风险和法律挑战。公司可通过电子邮件或智能手机随时联系雇员，工作和休闲时间之间的界限变得越来越模糊，那么我们如何保护雇员？我们如何在提供灵活工作时间的同时，确保对客户要求的实时响应？

工作时间

欧盟《工作时间指令》(2003/88/EC) 规定整个欧盟的雇员保护最低标准（尽管一些国家已实施超过该最低标准的进一步措施）。

根据该指令，雇员的周工作时间平均不得超过 48 小时，每天至少连续休息 11 小时，每周休息 24 小时，并且每年必须至少享有 4 周的带薪休假。

但是，在如今的数字时代，典型的日工作 8 小时模式不再是常态，由于通过智能手机可随时联系雇员，工作时间和闲暇时间之间没有严格的区分。特别是休息时间最容易受到影响。例如，当晚上或周末雇员在家里检查电子邮件时，是否会中断强制性休息时间？这个问题通常并未得到解决，并且在什么情况下构成中断休

息时间并不明确。欧洲法院称雇员在休息期间不应受到任何义务的限制，确保他们能够不受干扰地自由控制享有的休息权。

实际上，为了获得更大的灵活性，大多数雇员愿意通过电子邮件接受下班后工作。从法律上讲，由于通过电子邮件随时联系的雇员并非随叫随到，因此在很大程度上这种情形不受管制。但是，法国在 2017 年实施一项最新的劳动法规定，其中限制下班后向雇员发送电子邮件，从而为其提供“离线权”。其他国家是否也会采用此举还有待观察。

家庭办公、自带设备和雇员监督

随着移动技术的发展，家庭办公正在迅速普及。但是如果雇员在家工作期间受伤如何处理？在这种情况下，投保私人意外保险是必不可少的。

在采用家庭办公模式时，由于主管无法直接监控雇员，雇主需更加信任雇员。这可能提高欺诈地记录工作时间或超过法定工作时限的风险。

一般而言，除劳动所需的基本数据以外，雇主不得收集或使用其雇员的私人数据。因此，如果希望监控雇员使用的 IT 设备，需考虑相关的法律问题。例如，使用工作用移动设备不断收集数据。如果雇主希望获得这些数据，则必须与职工委员会达成协议，如果没有职工委员会，则须与相关个人达成协议。否则会产生不遵守数据保护规则的潜在风险。

当允许使用业务工具（例如移动电话、笔记本电脑和电子邮件账户）进行个人通信和实施“自带设备”计划（允许在业务中使用私人通讯工具）时，这使得私人领域和工作领域之间的界限更加模糊。这还可能导致数据失控，从而引发与数据保护法的潜在冲突。为避免违反数据保护法规，雇员必须区分其私人数据和业务相关数据。

零工经济

数字技术已经产生一个不断增长的新式劳动市场，它经常被称为零工经济。这主要是指自由职业者从事短期工作，并且在媒体、广告、建筑、信息技术和交付/运输服务等领域很常见。产生零工经济的主要原因是出现能够将自由职业者与潜在短期工作机会相匹配的新技术平台，如优步和 Deliveroo 等。

这种工作安排越来越普及——无论是寻求短期协助的企业还是工人，他们更喜欢较为灵活和独立的工作安排。但是，它们也引起争议，由于雇主不支付社会保险费和工资税，工人无法得到最低工资、病假或限制解雇的保护。

由于独立承包商在类似的条件和政策下经常从事与普通雇员类似的工作，因此欧洲的许多法院倾向于将这种安排解释为劳动关系。因此，雇用自由职业者的公司可能被社会保障部门重新评估，或者工人到劳工法院向其提起索赔，以要求将双方关系重新界定为长期劳动关系。

由于这一新兴趋势，包括法国、荷兰和其他国家在内的一些国家正在制定法律，为自由职业者或短期工人提供更多保护，并要求雇主支付该等工人的社保费和/或保险费。

在工作中使用可穿戴设备

可穿戴设备（用户佩戴的移动计算机系统，例如智能眼镜或健身手环）是数字世界中的新兴趋势。在工作场所使用此类可穿戴设备时，它们通常会收集、处理和使用个人信息。这种可穿戴设备通常连接到个人用户账户，以将移动计算机系统生成的信息分配给特定雇员。一般而言，在这种情况下适用数据保护条款。

在工作场所使用私人可穿戴设备时可能产生问题。如果雇员处理敏感业务和公司机密信息，雇主可禁止在工作场所使用和佩戴智能眼镜。如果雇员可能使用其智能眼镜的相机或记录功能以获得公司机密和商业机密，则足以据此禁止他们在工作场所佩戴智能眼镜。

但是，如果使用这些可穿戴设备对雇员的工作绩效没有影响，并且与个人手表的情形相当，则雇主不得禁止在工作中使用或佩戴私人可穿戴设备。另一方面，如果可穿戴设备影响工作时间或绩效，则雇主可以禁止使用。

消息服务的专业使用

目前，全球有超过 10 亿的数字消费者每天使用 WhatsApp 或 Skype 等消息服务。雇主通过消息服务可以在工作和休息时间内快速且轻松地联系到雇员。它们在与客户和业务合作伙伴保持业务联系方面也具有优势。

服务提供商已承认这一趋势。例如，根据媒体报道，即将开发商业版本的 WhatsApp。但是，只有在进行数据保护以及防止未经授权访问的情况下，才允许使用消息服务。

雇员手机中的联系人列表定期记录有关其他雇员、客户和其他业务联系人的个人数据。从数据保护的角度来讲，雇主有责任保护这些信息。雇主必须确保其雇员的业务电话上的数据按照适用的数据保护法进行处理。对于《通用数据保护条例》（在第四章中已进行详细讨论）以及本地数据隐私立法而言，这可能产生问题。在最糟糕的情况下，如果不适当地使用消息服务，获得机密信息的律师或其他个人可能遭到处罚。

如果雇主通过向雇员提供技术工具和指示确保即时消息工具无法访问业务相关数据，则允许出于私用的目的在业务移动设备上使用消息服务。

社交媒体作为终止劳动合同的原因

一般而言，不得因雇员在工作场所以外的活动对其进行解雇。但是，如果雇员在社交媒体上发布辱骂、非法或不恰当的政治声明，那么这些声明不再受到言论自由的保护，并可能构成解雇的合法依据。在这种情况下，社交媒体上的信息须与劳动关系建立具体的联系，例如雇员在其 Facebook 个人资料上说明雇主名称。

云端的数据隐私

在短短几年内，许多企业在日常工作中已开始使用云端。作为发布政策和指令之合法权利的一部分，雇主通常可选择所使用的工作设备并发布指示。除职工委员会通常的通知和咨询权以外，在使用云解决方案时通常须与职工委员会共同作出决定。

结语

就技术进步而言，它并非“如果”的问题，而是“如何”塑造数字时代工作环境的问题。展望未来，我们面临的挑战是有效利用新技术带来的巨大机遇和优势，同时在将来保持高标准的雇员保护。

人工智能已成为日常生活的一部分：从文本和语音识别一直到定向在线广告和客户服务“机器人”。据预测，今年全球所有业务内容的 20% 将由机器编写，到 2020 年，人工智能机器人将为 85% 的客户服务互动提供支持。¹因此，在与数字消费者互动时，这是一个需要考虑的重要领域。

什么是人工智能？

人工智能是指表现出通常与人类（而非机器）相关行为的系统。最初是通过设计或编程来使机器执行任务，因此我们认为机器的能力有限。但是人工智能可从接收的信息中学习（例如通过物联网中的嵌入式传感器接收环境数据），并就提供的新数据作出不同响应。

1 Gartner, “2017 年及以后的十大战略预测：数字颠覆风暴”，2016 年 10 月。



人工智能 - 数字化转型的下一步发展

NICK GRAHAM AND MONIKA SOBIECKI, LONDON

总体而言，也可以认为人工智能展示出“智能”属性，这意味着它有能力完成复杂目标。²全球技术研究和咨询公司 Gartner 将人工智能定义为：.....通过学习、自行得出结论、理解复杂内容、与人类进行自然对话、提高人类认知表现（也称为认知计算）或取代人类执行非常规任务，看起来通常能够模仿人类表现的技术。³

机器学习

机器学习是一种流行的人工智能。它涉及开发使用输入数据的算法。在监督学习中，对数据进行标记，并有效地教导算法什么是正确答案。经过一段时间的算法训练后，可根据所教导的模式进行预测。在无监督学习中，不向算法提供标记数据，而是由设备自行寻找方法和创建模式，以处理接收的任何新数据。

欧盟委员会最近指出⁴，人工智能可以在传统模拟业务的数字化中发挥重要作用，并为许多项目提供大量资金，其中包括：

- 制造业：人工智能可预测智能工厂的维护和故障事宜。SERENA 使用人工智能技术来预测工业设备的维护需求。
- 农业：人工智能有助于提高生产率，减少昂贵肥料、杀虫剂和灌溉的使用，同时减少对环境的影响。MARS 是一种播种种子的移动机器人，工人可远程监控播种过程。

- 运输：人工智能可尽可能减少列车与轨道之间的车轮摩擦，最大程度地提高速度，并可实现自动驾驶。运输转型是一项涉及智能高速公路和主动轨道等提高效率的方案。

大数据和隐私

欧洲政治战略中心已确定近年来人工智能快速发展的三大因素——更强大的计算能力、更复杂的算法和大量数据的更高可用性。⁵

数据是运行人工智能的“燃料”，因此确保人工智能系统的可用数据集具有高质量且符合适用的隐私法律至关重要。人工智能隐私法的实际适用领域可能包括心理测试服务、员工招聘、监控技术以及零售商的客户洞察。

人工智能和《通用数据保护条例》

如第四章所述，《通用数据保护条例》规范个人数据的使用。在使用人工智能时，特别是在包含不同数据源的大型且快速更新的数据集（通常称为大数据）中部署人工智能，如果这些数据集包含个人数据，则会产生许多挑战。⁶

《通用数据保护条例》项下的合法处理

这些挑战之一是确保数据处理的公平、合法和透明。首先，这意味着针对人工智能正在处理其数据的数据主体，必须向其解释处理效果，特别是人工智能（包括分析）的使用涉及自动决策时。

2 Max Tegmark, 生命 3.0 - 人工智能时代的人类, Allen Lane, 2017 年

3 Gartner IT 术语表, <https://www.gartner.com/it-glossary/artificial-intelligence/>

4 数字单一市场：欧洲人工智能，欧盟委员会，2018 年 4 月 24 日

5 人工智能时代：迈向人本机器的欧洲战略，欧洲政治战略中心，2018 年 3 月 27 日

6 在 2017 年英国信息专员办公室发布的有关大数据、人工智能、机器学习和数据保护的文件中对这些问题进行更详细的探讨。

解决问题和提高效率 相比于单独使用人工判断，人工智能使公司能够作出更佳决策，或者充分利用有限的可用数据。在实践中有关这些发展和改进的一些实际示例包括：

- **客户服务：**亚马逊已部署神经网络，从而为客户提供个性化产品推荐，弥补其庞大产品目录与每个客户有限数据集（原因是任何个人通常购买的产品数量很少）之间的空白；⁷
- **医疗诊断：**CNN 或深度卷积神经网络（基于神经网络创建的人工智能系统）具备与皮肤科医生相当的能力水平，能够对皮肤癌进行分类。它可以在智能手机上运行，因此有可能为大众提供低成本诊断建议。⁸
- **网络安全：**麻省理工学院的计算机科学和人工智能实验室开发的人工智能2每天能够扫描和评估数千万日志行，并确定须提交给处理人员的任何可疑内容。人工智能2成功识别出 86% 的攻击，同时使分析师不必在误报上浪费时间和精力。⁹

通过确保发布适当的隐私声明，可部分地满足此要求。但是，公平和透明度比这个问题更为广泛，这意味着基于向其告知的内容，任何数据处理均应处于数据主体合理期望的范围之内。

其次，通过人工智能进行处理还必须存在适当的合法依据。如须取得同意，则该等同意必须是自由作出、内容具体和明确，并予告知。如果通过人工智能处理数据的情形并不明确，或者数据主体未充分了解处理的后果，则可能构成挑战。所有这些事宜都涉及采用创新和创造性方法来发布内容丰富且精心起草的隐私声明以及继续以有效方式为数据主体提供信息的重要性。

数据控制者和人工智能

数据控制者有义务确保他们遵守责任原则，这意味着他们必须遵守《通用数据保护条例》，并且必须表明其如何予以遵守。例如，他们必须确保通过设计和默认规则将隐私条款纳入系统之中，已实施适当的安全措施，并且在代表他们与任何第三方（例如提供人工智能技术的供应商）建立的处理数据合同关系中载有必要的强制性条款。在开始使用人工智能之前进行数据保护影响评估是协助识别风险和实施保护措施的重要措施。

如果数据完全匿名，则不再属于个人数据，因此不适用《通用数据保护条例》。但是，在存储到数据仓库中以用于训练算法之前，数据匿名化行为本身可构成处理形式，在这种情况下，应适用《通用数据保护条例》。公司需密切关注有关重新识别数据集的技术进步，确保任何匿名化处理仍然有效。

人工智能和其他数据法律

⁷ <https://aws.amazon.com/blogs/big-data/generating-recommendations-at-amazon-scale-with-apache-spark-and-amazon-dsstsne/>

⁸ <https://www.nature.com/articles/nature21056>

⁹ <https://www.wired.com/2016/04/mits-teaching-ai-help-analysts-stop-cyberattacks/>

人工智能技术中的数据使用将受到欧盟数字单一市场战略中进一步法律的监管，例如旨在消除非个人数据自由流动的障碍而即将出台的电子隐私条例以及有关非个人数据自由流动的最新拟议条例。欧盟委员会、欧盟理事会和欧洲议会于 2018 年 6 月 19 日就该条例达成临时政治协议。¹⁰

责任和安全

人工智能产品（例如物联网、人工智能机器人或者自动驾驶汽车和系统）可能产生责任问题。

实际示例可能包括智能家居或自动驾驶汽车。相关责任可能包括：¹¹

- 合同责任 - 基于消费者和零售商之间达成的合同。
- 严格责任 - 例如在欧盟层面基于在当地成员国实施的《产品责任指令》，当有缺陷产品对受害者造成损害（例如人身伤害、死亡或财产损害）时适用于“生产者”的严格责任制度。
- 过错责任 - 例如根据当地法律（如英国的过失法）。

“欧盟安全框架”包括许多指令，例如《机械指令》、《无线电设备指令》、《产品责任指令》和更详细规则，例如医疗设备和玩具。针对开发或者投放于市场的任何人工智能产品应考虑这些因素。欧盟委员会目前正在根据技术发展评估欧盟安全框架，以确定是否需要实施进一步监管。¹²

10 <https://ec.europa.eu/digital-single-market/en/free-flow-non-personal-data>

11 基于欧盟委员会工作文件的类别 - 新兴技术责任 (SWD (2018) 137)，2018 年 4 月 25 日。

12 从欧盟委员会至欧洲议会、欧盟理事会、欧洲经济和社会委员会以及地区委员会的沟通 - 欧洲人工智能 (COM (2018) 237)，2018 年 4 月 25 日。

13 同上，脚注 52。

14 2018 年 3 月出版的《有关人工智能、机器人和“自动”系统的声明》。

知识产权

在第八章中，我们探讨在数字环境中行使知识产权的挑战。使用人工智能创作作品也可能对知识产权产生影响，例如可申请专利性、版权和所有权。¹³当使用人工智能来创建或丰富公司希望保护的数据库或者培训人工智能来使用此类数据库时会产生这个问题。

人工智能监管的未来

有关人工智能的法律仍处于变动之中。尽管已制定有关产品安全和个人数据保护的监管框架，但是目前尚未对人工智能系统本身的开发和算法内容进行监管。

不过目前已在欧洲层面提出制定道德框架的提案。通过与欧洲科学和技术伦理小组的合作，预计到 2018 年底会拟定指南草案，该小组已开始在该领域开展工作。¹⁴

数字化转型的下一步发展

人工智能和人工智能技术的使用为探索数字世界的企业提供无与伦比的机会，从而利用其数据资源并在内部创造效率（例如员工参与或维护设备）。它还可以在接触数字消费者方面产生新的优势，例如在发布广告方面作出更佳判断，或者提供更佳的新式人工智能产品。无论公司如何使用人工智能，它必将改变商业世界，甚至超出我们的预期。

监管机器人和人工智能

机器人和人工智能的普及给社会和法律制度带来许多挑战。随着机器人开始渗透到生活的各个方面，我们需要预测潜在挑战，并开发法律如何监管人机关系的方法。世界各地的许多提案都试图回应这一需求，包括艾斯罗马人工智能 23 原则和欧洲机器人宪章等。

2016 年，Dentons（大成）受 Grishin Robotics 委托编制俄罗斯第一部机器人法草案。在定义相关概念时，团队不仅参考判例，还从科幻小说中寻找灵感，包括艾萨克-阿西莫夫的机器人法则。由此产生的文件引发人们对监管这一新兴技术领域的争论。

第二年，Dentons（大成）团队通过从全球视角审视这个问题，决定借鉴这一经验并进行更为全面的思考。由此在首个有关机器人的国际大会上发表一部草案，其中包括监管与网络实体系统的积极发展相关的人类关系 42 条规则。

该协定包括一套规则，其将当前已有的监管人工智能和机器人的所有方法结合在一起，包括有关机器人的“黑匣子”和“红色按钮”、安全和机密性问题以及机器人识别。它们还包括确定一种高风险机器人的新提案。最后，该协定审查人工智能和军用机器人的监管问题，以及在不同国家开发机器人技术方面的国际合作问题。

就该协定而言已在商业、学术和政治界进行辩论，发表于学术期刊上，并作为提案发送给联合国。

此外在 2017 年，Dentons（大成）律师协助建立致力于监管人工智能和机器人的 Robopravo 研究中心。该中心已制定若干法律草案，并出版有关新技术监管的期刊。





Contributors



Tímea Bana

布达佩斯辩护律师

电话 +36 1 488 5200

timea.bana@dentons.com



Yana Chirko

圣彼得堡辩护律师

电话 +7 812 325 8444

yana.chirko@dentons.com



Stefan Dittmer

柏林合伙人

电话 +49 30 2 64 73 390

stefan.dittmer@dentons.com



Matthias Eggert

慕尼黑合伙人

电话 +49 89 244408 487

matthias.eggert@dentons.com



Marc Elshof

阿姆斯特丹合伙人

电话 +31 20 795 36 09

marc.elshof@dentons.com



Sven-Oliver Friedrich

法兰克福合伙人

电话 +49 69 45 00 12 201

sven.friedrich@dentons.com



Tünde Gönczöl

布达佩斯辩护律师

电话 +36 1 488 5200

tunde.gonczol@dentons.com



Anastasia Gracheva

圣彼得堡律师助理

电话 +7 812 325 8444

anastasia.gracheva@dentons.com

**Nick Graham**

伦敦合伙人

电话 +44 20 7320 6907

nick.graham@dentons.com

**Hanna Karoline Heidkamp**

法兰克福资深律师

电话 +49 69 45 00 12 148

karoline.heidkamp@dentons.com

**Frank Lenzen**

法兰克福合伙人

电话 +49 69 45 00 12 284

frank.lenzen@dentons.com

**Svetlana Lialkova**

圣彼得堡律师

电话 +7 812 325 8444

svetlana.lialkova@dentons.com

**Shane Mercer**

多伦多全球商业技术总监

电话 +1 416 361 2313

shane.mercer@dentons.com

**Igor Ostrowski**

华沙合伙人

电话 +48 22 242 56 73

igor.ostrowski@denons.com

**Christoph Papenheim**

法兰克福合伙人

电话 +49 69 45 00 12 201

christoph.papenheim@dentons.com

**Georgy Pchelintsev**

圣彼得堡合伙人

电话 +7 812 325 8444

georgy.pchelintsev@dentons.com



Constantin Rehaag

法兰克福合伙人

电话 +49 69 45 00 12 248

constantin.rehaag@dentons.com



Kseniia Smirnova

圣彼得堡律师助理

电话 +7 812 325 8444

kseniiia.smirnova@dentons.com



Monika Sobiecki

伦敦律师

电话 +44 20 7320 6089

monika.sobiecki@dentons.com



James Venit

布鲁塞尔合伙人

电话 +32 2 552 2941

James.venit@dentons.com



Natalia Selyakova

基辅合伙人

电话 +380 44 494 4774

natalia.selyakova@dentons.com



Victor Naumov

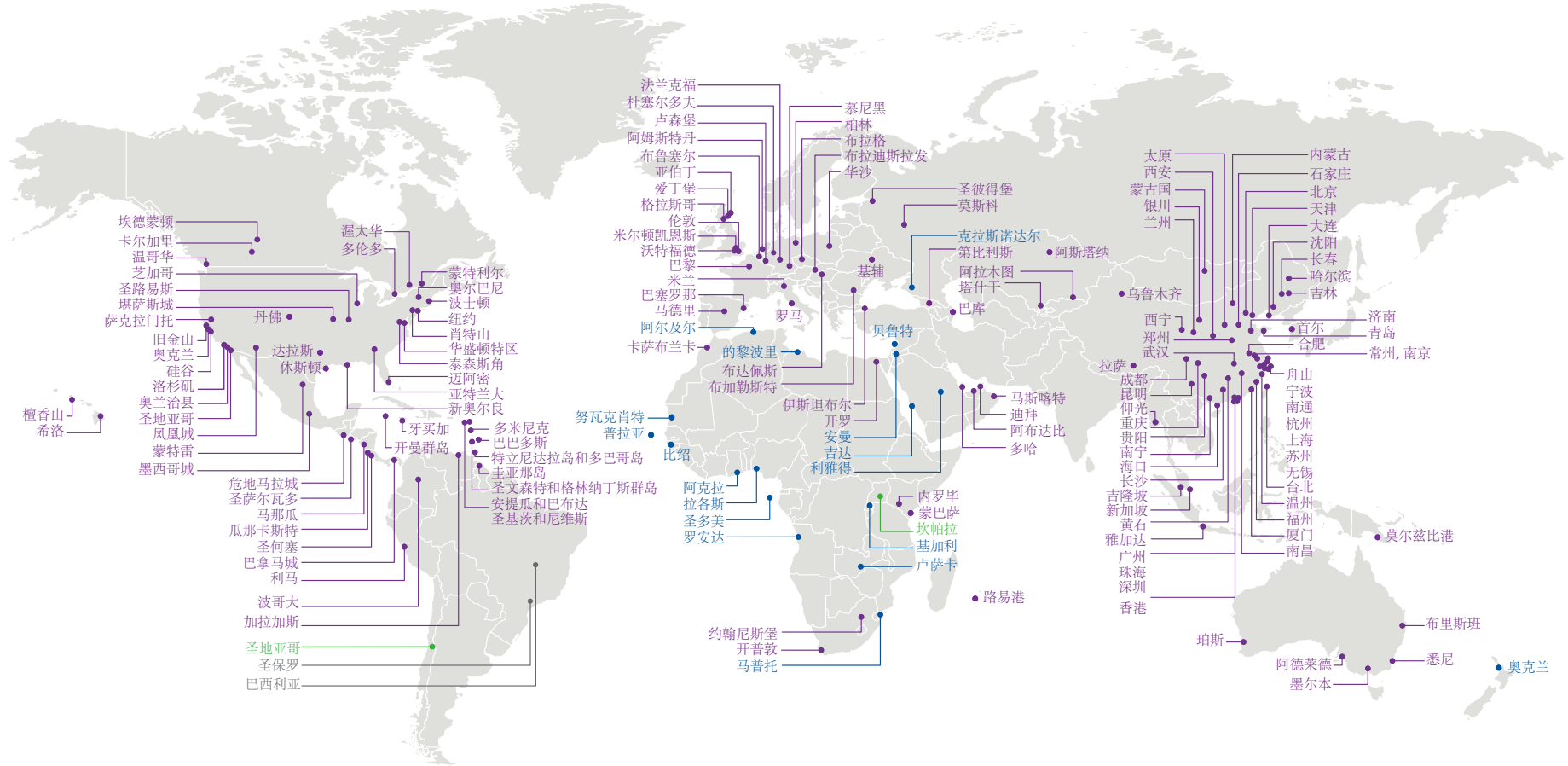
圣彼得堡合伙人

电话 +7 812 325 8444

victor.naumov@dentons.com

欧洲的技术、媒体和电信

Dentons（大成）的技术、媒体和电信 (TMT) 业务提供全方位的法律建议，从普通的并购和企业咨询到更专业领域，例如监管问题、IP/IT 许可和分销协议以及国际频谱分配。我所在欧洲聘有 150 多名 TMT 律师，在全球聘有 450 多名 TMT 律师，在开展业务的任何关键市场，我所均可为团队提供宝贵的拓展支持。[注意：地图不需要翻译，我们已有相应的译文]



紫色显示的地区代表大成办公室。
蓝色显示的地区代表关联律所、办公室和特别联盟律所。
绿色显示的地区代表拟议合并但尚未正式生效。
灰色显示的地区代表巴西战略联盟。

► Dentons（大成）是世界上最大的律师事务所，致力于为全球客户提供优质服务和价值。Dentons（大成）是 Acritas 全球精英品牌指数中的领导者，曾获得 BTI 客户服务 30 强奖项，以其创新性客户服务得到了多家知名商业和法律出版物的认可，并创建 Nextlaw 实验室和 Nextlaw 全球推荐网络。Dentons（大成）采用多中心方法，拥有众多敢于挑战现状的世界一流人才，帮助客户在其生活和工作的社区中获得更大利益。

dentons.com