

《欧盟一般数据保护条例》背后隐含的伦理层次

张志杰 201721040843

摘要：本文通过《一般数据保护条例》(GDPR)的推出和即将生效，对人工智能应用于商业的方式彻底整改引发了 AI 社区和技术巨头的激烈争论这一例子引出了数据时代涉及到的一些伦理问题。通过对 GDPR 的部分条例的阐述，技术巨头的看法，引出其背后所隐含的伦理方面的知识以及面对鱼与熊掌时，科技发展与隐私该如何取舍？

关键字：数据保护；隐私；科技；伦理

1 引言

《一般数据保护条例》是 20 年来数据隐私条例的最重要的变化，它将取代《欧盟个人资料保护指令》，并将协调全欧洲的数据隐私法律，为所有欧盟民众保护和授权数据隐私，并将重塑整个地区的数据隐私保护形式^[1]。

信息时代的发展，大数据、云计算、移动互联网、社交网络以及各种智能终端的普及使得个人数据无处遁形，而自然人的天然弱势地位导致其难以掌控自身数据，故此 GDPR 的推出使得应对数字时代个人数据的挑战有法可依，从而维护自身权利。

从这个例子我们必须了解到大数据信息时代的伟大和便宜性是毋庸置疑的，科技的进步带来广泛的好处是有目共睹的。但是不可否认也伴随着在光辉成就面具下的潜藏危险性，包括隐私权，社会公平以及自身安全等等。

本文组织结构如下：第 2 节阐述了《一般数据保护条例》的部分条例规则，以及对其的辨析；第 3 节通过科技巨头的争论引出科技发展与隐私保护的争锋；第 4 节通过这个例子折射出的工程伦理的一些思想；第 5 节是对例子延伸的思考。

2 条例的具体分析

GDPR 明确指出符合条例的企业反思其条款和条件(解释该公司如何使用个人数据来销售广告)中的内容, 强制企业遵循 **privacy by design** 原则^[3]。

- 数据转移权: 该规定声明, 用户可要求自己的个人数据畅通无阻地直接迁移至新的提供商。数据以机器可读的格式迁移。

这个原则对于个人而言显然保障了对个人数据有更多的掌控权, 人们可以自由控制个人信息数据的流动, 可以优雅地从网上“消失”; 但是对于企业来讲, 特别是对于谷歌、Facebook 等名副其实的数据挖掘公司和较小的数据科学创业公司而言, 这就像是敲响了丧钟, 当用户不再使用该公司产品时, 它们将会丢失大量数据。

- 被遗忘权: GDPR 第 17 条强调, 每个数据主体有权要求数据控制者删除个人数据, 并且不能过分延长数据留存时间, 控制者有义务遵循该规定。
- 决定权: 数据主体可以要求自主决策权, 即使企业提供自动选择或决策服务

这两个原则体现了个人的自主权利得到更多的保障, 可以自主决定个人数据信息的去留, 维护自身的权益。通俗点说即为社交网络公司在使用你的数据之前必须征得个人的同意, 例如商家不能再随意地发送推广邮件。相反地, 这就对以 **cookie** 形式收集数据, 从定向投放广告中获取收益的技术巨头而言就是一项巨大的损失。

- 算法公平性: 自动决策的可解释权指出数据主体有权要求算法自动决策给出解释, 有权在对算法决策不满意时选择退出。

显然，对个人来讲会更加的透明化，明确清晰地了解个人数据信息的情况，例如申请贷款或者网上求职时，被系统自动决策拒绝时，此时有权寻求解释，找出拒绝原因而并非其他潜规则因素导致，维护了个人权益。但对于当下火热的 AI 智能技术无非是一次巨大的打击，这是对 AI 的严重限制，将大幅减缓 AI 技术的发展。

下一节具体阐述了隐私保护与 AI 发展的矛盾争锋。

3 科技发展 or 隐私保护

目前被广泛应用的人工智能技术可谓是如火如荼，是人工智能史上的第三高峰。但是其中的深度学习及其不可解释性(即黑箱状态)显然违背了算法公平性中的解释原则，这可能会导致任何的 AI 公司无法开展已有业务。

目前由于 GDPR 法案的颁布，腾讯发出公告，QQ 国际版将暂时停止在欧盟的服务^[2]；《终极算法》作者，华盛顿大学教授 Pedro Domingos 在社交网络中说道：自 5 月 25 日起，欧盟将会要求所有算法解释其输出原理，这意味着深度学习成为非法的方式。

显然，GDPR 的相关法规跟现代科技技术有着不可避免的冲突，尤其对于人工智能方面。人们对于神经网络的最大批判是：

- 缺乏可解释力，我们无法确定隐藏层内部发生了什么。但是神经网络在近似值和精确度上普遍得分较高
- 在现实世界中很难解释摘要权重，但是在传统技术中却不是，这进一步加深了黑箱难题

那么是否要遵循 GDPR 条例，在解决深度学习的黑箱难题之前限制 AI 公司的发展呢？在当下科技领域尝到了 AI 智能技术的甜头，如 AlphaGo、无人驾驶

等等引领 AI 智能的新科技已经带给人们巨大冲击和好处的前提下，限制其发展是否会堵塞科技的进步呢？这显然是一对矛盾体。是选择科技发展带来的便宜生活还是维护自身的隐私权利？在本文看来并非不可兼得，首先，AI 智能的创新显然会是引领科技潮流的一股生力军，这将会是这个世纪科技飞速发展的起点，其次对于隐私保护也是不容忽视，需要在发展 AI 智能的同时，加强创新人才隐私安全保护的意识以及完善相关互联网隐私维护、问责机制，双管齐下，逐步完善完美的科技力量。

4 涉及到的工程伦理思想

工程伦理学是当下接受的、各个工程师组织和工程协会所批准的用以指导工程实践的道德价值、行为准则和道德标准以及工程师个人的道德思想、品质、观念和行爲，解决工程中道德问题以及论证与工程有关的道德判断的活动和学科。本文将从工程伦理中的对立观点以及解决伦理问题的原则和方法两方面进行阐述^[4]。

4.1 工程伦理观点：技术自主论与工程工具论

法国哲学家埃吕尔、莱姆等认为技术是自由的技术发展不受外界(包括伦理道德)的控制，这就是技术自主论。它推崇技术自主发展和人类的自主性和人的选择行爲是不相容的，伦理道德不可能约束技术的发展；而恰恰相反，技术作为一种推动社会变革的力量，决定和支配人的道德和社会状态。

在技术自主论中，反映出 GDPR 的推出是完全没有必要的，即使你执意推行 GDPR，对于科学技术的发展也是无法构成影响的，因为它认为技术是不受外界任何因素的控制而有所改变，技术只会按照它自己的节奏继续发展，更有甚之，人类必须去适应它而有所改变，也就是说，在大数据时代，人们必须习惯自身隐

私数据被他人所知这一事实，可想而知，这一事实会造成多大的后果，这对于现阶段非所谓的理想世界来说甚至无法面对整个世界。因此技术虽然具有一定的独立性，但归根到底是由人来承担和进行的，人的技术拥有决定和选择的能力。

因而德国哲学家雅斯贝尔斯提出了工程工具论，技术只是实现人类某种目的的手段这一观点推翻了对技术自主论的本质。技术不但产生人们所希望的结果，还可能产生人们目的和期望之外的或好或坏的结果，例如氟利昂的生产和使用、大数据时代数据泄露的隐患等。技术对人的观念具有反作用，这一点也跟技术自主论有所差异，技术会影响人但无法决定支配人类。技术的强化趋势会造成连锁的社会和环境效应，技术本身具有鲜明的善或恶的价值倾向。

工程既然是一种手段，在工程活动中对人的观念具有反作用力，那么在工程活动的每个阶段都会存在伦理问题，工程内涵着某些超出事先预料、或好或坏的结果。而在解决工程伦理问题时，就需要有相对应的原则和方法。

4.2 解决原则和方法：功利主义原则和尊重人的伦理学原则

功利主义思考方式倾向于带给我们所能得到的最大整体利益，对受到其影响的人产生最大的整体效用。那些个体行为或规则是正当的。在这种原则下 GDPR 的推出是否正确就值得商榷了，原因在于一旦全面实施了 GDPR 法案，那么大量的科技巨头公司就会停止对外的互联网业务，科技发展必然受到严重的打击。试想一下，当下互联网的覆盖率基本遍及全世界的每个角落，一旦停止了互联网的业务，就相当于遮住了全世界网民的眼睛，造成的损失将是无法估计的。再拿经历三起三落的人工智能技术来讲，近几年 AI 技术飞速发展，AlphaGo、无人驾驶等 AI 技术已经崭露头角，前景一片大好，甚至最终可能达到人类能力的又一里程碑，但是此时由于 GDPR 的相关规定使得 AI 技术发展滞留，不再创新发

展，这显然因小失大，只顾当下而不顾大局。

当然，功利主义的立场也会面临诸多困境：从功利主义立场出发很难提出一种行动方向；无法准确确定最大受益群众的范围；有时会对个体带来不公正的行为辩护。

这时就需要顺从尊重人的伦理学原则，其道德标准就是我们所遵守的行为或规则应当把每个人都作为相互平等的道德主体来尊重。GDPR 的起案标准就是基于尊重个人的原则，把每个人的数据信息保护写进法案法规，切实维护做到有法可依。虽然可能会造成某些利益的损害，但是应该更注重个体利益，维护隐私权，这是个人最基本的权利。

5 延伸思考

在本文看来，那么是否就完全按照尊重人的伦理原则实施 GDPR，亦或是反对 GDPR 而站在功利主义上呢？功利主义的立场积极并有前瞻性，尊重人的伦理立场更具有保护性，站在二者之一都显得有点因小失大，太过片面。站在本文角度，更加倾向于在科技发展的同时兼顾个人隐私的保护，例如可以实施以下的措施：

- **个体隐私保护意识加强。**在互联网世界上保持警惕，不随意打开陌生网站，尽量保留个人信息，浏览可信度较高的网站，安装杀毒软件和防火墙，定期清理浏览记录。
- **相关部门实施法案法规。**例如 GDPR，但是可以针对个别部分根据实际情况区别对待，例如 AI 技术现阶段无法实现程序处理透明化，不应完全否定禁止，可以建立监督问责机制，实施监控同时又不阻碍其发展，另外可以设立专门研究部门研究解决其黑箱状态，实现利益最大化。

- **科技公司和开发人员应具有职业操守。**既不多要本身服务不需要的用户数据，又要保护本身已获得用户数据的安全，绝不贩卖或做任何侵犯用户隐私权的事情。作为公司，本身具有网络保护的實力，应将保护公司商业机密的决心用在保护用户隐私上。

参考文献

- [1]. 知乎 “机器之心”专栏 深度学习即将非法？欧盟《一般数据保护条例》五月生效
- [2]. 知乎：如何看待欧盟颁布的《一般数据保护条例》
- [3]. GDPR 官网 <https://www.eugdpr.org/>
- [4]. 河北工程大学工程伦理学课件
<https://wenku.baidu.com/view/c616fee47375a417866f8fec.html>