디지털 신원 관리에 대한 책임

Mike Donoghue - 2019 년 6 월 28 일

주제: **Business Intelligence, Digital Project Management, Innovation**

기술과 접근(접속) 측면에서 볼 때, "가진" 사람들 과 "가지지 않은" 것으로 간주되는 사람들이 있습니다. 일부 개인은 품질이 낮은 상품과 서비스(예를 들어, 연결성)로 어느 정도 어려움을 겪는 경우도 있지만, 수입, 교육, 나이, 지리적 환경 및 기타 요인의 차이로 박탈감을 느끼는 사람들도 분명히 있습니다. 그리고 이는 디지털 격차를 유발합니다.

"디지털 격차"라는 말은 광범위하고 복잡하며 정치적으로 사용될 수 있으므로 National Digital Inclusion Alliance (미국 기반 비영리 단체)는 "디지털 통합"이라는 용어를 사용하는 것이 더 적절하다고 말합니다.

디지털 통합*은 가장 불우한 사람들을 포함하여 개인과 공동체가 정보 통신 기술에 접근성과 사용권을 가지는 것을 확실히하는데 필요한 활동을 말합니다.*
이것은 다음의 5가지 요소들을 포함합니다.

1. *저렴하고 원활한 광대역 인터넷 서비스*
2. *사용자들의 요구를 충족시키는 인터넷 사용 가능 장치*
3. *디지털 문맹 개선에 대한 접근*
4. *품질 기술 지원 그리고*
5. *자급자족, 참여 및 협력을 장려하고 가능하도록 고안된 어플리케이션 및 온라인 콘텐츠*

디지털 통합은 기술 발전에 따라 성장해가야 합니다. 이를 위한 기술적 접근 및 사용에 대한 역사적, 제도적 그리고 구조적 장벽을 줄이고 제거하기 위한 전략과 투자가 필요합니다.

디지털 통합과 궁극적인 기술 평등 촉진의 열쇠는 ID 즉, 신원의 개념에 있습니다. 가장 순수한 의미에서 신원이란, 우리가 개인으로서 누구인가 -우리가 액세스할 수 있게 허용된(허용되지 않은) 상품, 서비스 정보를 포함해서– 하는 것입니다.

디지털 세계의 기하급수적인 성장은 전반적으로 보다 많은 기회 창출을 가능하게 하였으나, 우리가 그룹 및 개인으로 분류되어 소외될 가능성이 있으며, 디지털 프로파일로 인해 분리되거나 사라질 위험이 있습니다. 우리는 예전보다 더 긴밀히 연결되어 있기 때문에 우리에 관한 정보가 더 많이 제공될 수록 취약해질 수 밖에 없습니다. 그리고, 우리가 누구인지, 어떻게 나타나는지 분석하고자 하는 사람들이나 도구들에게 통제 당할 수 있게 됩니다. 물론, 반드시 연결을 끊은 상태로 있는 것이 해결책이 되는 것은 아닙니다. 디지털 참여의 부족이 더 많은 배타적인 결과를 초래하

기 때문입니다.

우리의 디지털 정체성을 관리할 능력과 의지를 갖는 것이 이익을 얻는 사람들과 그렇지 않은 사람들의 격차를 좁히는데 중요합니다. 온라인 즉, 연결된 세계에서 개인과 조직/기관 간의 강력한 관계 형성에는 선택과 신뢰, 특권 및 보호가 중요합니다. 이러한 능력과 접근의 자유가 개인의 디지털 미래를 위한 기반을 조성할 수 있는 경제적, 정치적, 사회적 기회를 증진시키데 필수적입니다.

우리가 데이터 중심의 세계로 접어 들면서, 우리의 신원이 디지털 요소와 밀접하게 연결되었다는 것을 알 수 있습니다. 가령, 기업, 정부나 다른 기관에서 거래 및 교환 업무를 하려면 검증 가능한 디지털 신원을 사용해야 합니다. 안전, 보안 및 인식의 목적으로서 공개적 신원확인은 디지털 프로파일과의 연결을 요구합니다.

디지털 정체성이 각 개인으로서의 우리에게 중요한 가치를 제공하기 위해 지니고 있어야 하는 기본적이지만 필수적인 기능이 몇 가지 있습니다.

- **신뢰와 확실성**: 강력한 디지털 정체성을 지닌다는 것은 자신과 다른 사람의 신원확인을 도와줄, 신뢰할 수 있는 프로세스가 있다는 확신을 갖는 것을 의미합니다. 강력한 디지털 정체성을 갖는 것은 적합성과 접근 관행을 위해 필수적입니다.
- **열린 접근**: 디지털 정체성은 개인적 데이터(인구 통계 등)에 따른 편견이나 차별로부터 자유로워야 하며 배타적이지 않은 신원확인 절차가 뒷받침되어야 합니다. (즉, 개인이 의도적으로 차단되지 않도록 해야합니다)
- **가치성**: 디지털 정체성을 유지하는 것이 가치있어야 한다. 특히, 도움이 되는 중요한 서비스 및 연결(예를 들어, 구매 및 통신)에 쉽게 접근하고 사용할 수 있는 기능을 제공해야 합니다.
- **선택권**: 디지털 정체성에 대한 일종의 개인 소유권이 있어야 하며, 이는 시스템에게 정보 공유 여부에 대한 우리의 권리를 행사하는 것으로 공유할 수 있는 정보의 양, 방법, 대상 및 정보의 기간을 포함합니다.
- **보호**: 디지털 정체성은 공격에 취약합니다. 남용되거나 부적절하게 사용되는 경우, 개인, 조직, 기술 및 인프라 구성요소가 손상되어 잠재적으로 프라이버시 및 보안 위반 그리고 기타 불법행위를 초래 할 수 있으므로, 안전하게 지켜져야 합니다.

이러한 기능들은 모두 우리를 인식하고 누구인지 확인할 수 있는 시스템에서의 우리의 존재와 관련 있습니다.

오늘날의 기술에 있어서 정부나 기업과 같은 기관들은 전통적이고 중앙 집중적인 방식에 기반한 자체시스템에 디지털 정체성(관련된 정보와 더불어)을 만들고 유지해 나갑니다. 다행히, 또 다른 신원확인 시스템은 새로운 설계 방식을 따르는데, 이는 보다 분산된 방식, 덜 중앙 집중적으로 개개인에게 자신의 디지털 신원 자료에 대한 더 많은 통제를 부여합니다.

미래에 디지털 정체성을 가진 사람들을 돕고 평등 중심의 커뮤니티를 형성하기 위해 즉각적인 관심과 집중을 기울여야 할 부분들이 있습니다:

- 디지털 정체성 네트워크를 감독하는 방법에 대한 신규 모델 창안
- 훌륭한 신원 원칙을 지원하는 개발 도구 및 책임 가이드라인 개발

핵심은 심층적 검색의 필요성과 더 나은 디지털 정체성 감독의 방법을 모색할 때까지 우리가 얼마나 자신을 밝힐지 그리고 이에 따르는 위험이 무엇인지를 결정하는 것입니다.

디지털 세계에서 지침과 규정의 부재 시, 기회주의자들은 불균형을 조성하고 불평등을 조장할 것입니다.