Journal of the The Korean Institute of Defense Technology Vol. 05, No. 3, pp. 001-007, 2023

국방 분야 인공지능 기술 접목에 따른 교육훈련 데이터 가명처리 방법론에 관한 연구

A Study on the Data Pseudonymization Methodology for Defense Training Data as Artificial Intelligence Technology is applied to the Defense Field

조현석*,1) . 강수진1) . 조동래1) . 신영섭1)

Hyunsuk Cho*,1) . Sujin Kang1) . Dongrae Cho1) . Yeongseop Shin1)

[초 록]

최근 국방 분야에서는 인공지능 기술을 접목하기 위해 데이터센터를 구축하여 데이터를 모으려 한다. 무기체계 훈련 데이터는 인공지능 모델의 입력 데이터로 사용되어 훈련 성과를 극대화하고 군 전략을 발전시킬 수 있는 양질의 데이터로 사용될 수 있다. 하지만 훈련 데이터에는 그 장비를 운용했던 인원의 이름과 군번 등의 개인적인 정보와 무기체계의 특징을 알 수 있는 훈련 기록들을 담고 있다. 이런 데이터가 적군에게 넘어간다면 무기체계의 제원 및 성능뿐만 아니라 운용자별 숙련도도 노출될 수 있다. 본 논문에서는 교육훈련 데이터 보안을 위해 가명처리 방법론을 제안하고 관련 법령의 개정 방향도 제언한다.

[ABSTRACT]

Recently, in the defense field, efforts are being made to collect data by building data centers to incorporate artificial intelligence technology. Weapon system training data can be used as input data for artificial intelligence models and can be used as high-quality data to maximize training performance and develop military strategies. However, training data contains personal information such as the names and military numbers of the personnel who operated the equipment, and training records that reveal the characteristics of the weapon system. If such data is passed on to the enemy, not only the specifications and performance of the weapon system but also the proficiency of each operator may be exposed. In this paper, we propose a pseudonym processing methodology for education and training data security and also suggest a direction for revising related laws.

Key Words : Weapon System(무기체계), Training Data(훈련 데이터), Privacy(개인정보), Pseudonymization(가명처리)

1. 서 론

현대의 첨단 무기체계는 과거 재래식 무기와 다르게 여러 구성품들이 모여 하나의 무기체계로 구성된다. 또한 기술의 발전과 무기체계 내에 소프트웨어의 비중이 높아지면서 무기체계를 운용하는데 복잡하고 어려워졌다. 이에 따라 군은 무기체계를 운용하는 데 있어 많은 교육훈련과 숙련 과정이 필요하게 되었다. 무기체계 교육훈련장비는 과거 재래식 무기의 단순한 교보재가 아니라 전시 상황을 모의하여 실제 전투 상황에서 무기체계 운용을 훈련할 수 있도록 발전하였다. 교육훈련장비의 분야 또한 전투기부터 현재 대두되고 있는 사이버 공간의 사이버 공방훈련장까지 다양하다.

국방 분야에서는 지난 2023년 1월 31일 데이터 중심의 군 환경을 구축하기 위해 '국방데이터분석센터'를 개소하였다. 국방 데이터 현황 관리, 데이터 수집 사업 추진, 데이터 표준 및 품질 관리, 데이터 관리·활용 등과 관련하여 국방부와 각 군을 지원하는 역할을 수행 할 예정이다.[1]

무기체계 교육훈련 장비를 이용하는 운용자는 훈련 결과를 데이터로 저장한다. 이 데이터에 인공지능 기술을 접목하면 무기체계 성능 개선뿐만 아니라 각 군의 전술 및 전략을 발전시

1) LIG넥스원 C4ISTAR연구개발2본부 (C4ISTAR 2nd Research & Development, LIG Nex1)
* Corresponding author, E-mail: ambitihyun@naver.com

Received : August 26, 2023 Revised :
Accepted : September 22, 2023

킬 수 있는 양질의 데이터로 사용될 수 있다. 데이터 중심의 군 환경을 구성하고 무기체계 훈련 데이터를 한군데 모을 수 있다면 그 이점은 배가 될 수 있다. 또한 훈련 대상자 입장에서도 훈련 데이터를 인공지능 모델로 분석하면 훈련 결과에 대한 피드백 수준을 높일 수 있어 훈련 효율을 극대화 할 수 있다. Kim et al.[2]에서는 교육훈련분야 중 의사결정 지원체계, 지능형 교관, 가상 개체 자동 모의 분야를 대상으로 인공지능 기법을 적용해보고 구체적인 발전 방안을 제시하였다.

문제는 이 훈련 데이터들이 데이터 보호 관점에서 바라봤을 때 전혀 보호되고 있지 않다는 점이다. 비록 군이라는 환경의 특수성으로 인해 물리적인 데이터 유출이 어렵고, 무기체계 운용자의 개인 정보는 운용을 위한 최소한의 인적자료라는 점에서 문제가 되지 않을 수도 있지만 이 정보가 적에게 유출되었을 경우는 상황이 다르다. 훈련장비에 입력되는 운용자의 정보는 소속과 이름, 계급 및 군번 등으로 누가 어디에 소속되어있고 작계지역은 어디인지까지 알 수 있다. 또한 각 훈련장비 운용자는 훈련된 데이터로 무기체계 숙련도뿐만 아니라 상황에 따른 운용자의 조작 습관도 파악할 수 있다. 이러한 정보가 적군에 들어간다면 전시에 무기체계 운용자에 따라 맞춤형 대응을 할 수도 있고 평시에도 숙달된 운용자의 신변이 위험할 수 있다.

무기체계 훈련장비의 운용 환경은 대부분 망에 연결되어 외부 공격자로부터 침입이 불가능해 훈련 데이터가 유출되지 못한다고 생각할 수 있지만 최근 대두되는 군사 비밀 유출은 군 내부자에 의해 발생한 케이스가 많다. 국방통합데이터센터에 업로드 된 훈련 데이터 또한 외부의 접근 권한이 없다고 해도 내부자에 의한 데이터 유출 상황은 배제할 수 없다. Eom et al.[3]에 따르면 군 내부정보 유출에 대한 다양한 케이스를 소개하고 대부분의 유출 경로는 내부자로 인해 발생하기 때문에 내부자 행위에 중점을 두고 정보유출 방지 방안을 제시하였다. 또한 Kim et al.[4]은 스파이 칩 등을 이용하여 망분리가 된 환경에서도 충분히 데이터를 탈취해갈 수 있다고 소개하였다.

2020년 데이터 3법 개정으로 개인정보보호법에 포함된 가명정보는 가명처리를 통해 특정 개인의 정보를 알아 볼 수 없도록 처리되었다. 이 가명처리 기술을 군 교육훈련장비에 이용하면 무기체계 운용자 및 운용 환경 정보가 외부로 노출되지 않으면서 인공지능 기술을 이용할 수 있다. 따라서 본 논문에서는 군 환경에서 무기체계 교육훈련 데이터를 가명처리하는 방법을 제안하여 인공지능 기술을 접목할 때 보안 확보 방안을 제시한다.

본 논문은 서론에 이어 2장에서는 본 연구와 관련된 용어를 정의를 하고 3장에서는 관련 연구를 소개하며 4장에서는 무기체계 훈련장비 가명처리 방안을 제시한다. 5장에서는 법체계 정합성을 위한 제언을 하고 마지막 6장에서는 기대효과 및 향후연구를 논하고 논문을 마무리 한다.

2. 용어 정의

2.1 가명정보

앞서 언급한 바와 같이 가명정보는 데이터 3법 개정으로 새롭게 탄생한 개념이다. 개인정보보호법에서는 그 정의를 '개인정보를 가명처리 하여 원래의 상태로 복원하기 위한 추가 정보의 사용·결합 없이는 특정 개인을 알아 볼 수 없는 정보'로 내리고 있다.[5] 즉 가명정보의 목적은 데이터 안에 있는 개인정보를 가명처리해서 타인이 알아보지 못하게 하는 것이다. 가명정보는 익명정보와 마찬가지로 개인의 정보가 일부 삭제되거나 다른 정보로 대체되지만 가명정보는 추가 정보를 이용하여 원래 정보로 복원이 가능하다는 차이점이 있다.

2.2 데이터 결합

하나의 데이터로는 특정 개인을 알아볼 수 없더라도 다른 정보와 결합하면 개인정보가 노출될 수 있다. 이렇게 서로 다른 데이터를 합치는 행위가 데이터 결합이다.

가명정보는 통계작성, 과학적 연구, 공익적 기록보존이 목적인 경우 개인의 동의 없이 활용이 가능하다. 가명정보는 다른 가명정보와 결합될 때 그 가치는 더욱 높아질 수 있다. 그러나 서로 다른 개인정보처리자가 데이터 확보를 위해 보유하고 있는 정보를 직접 결합해서는 안 된다. 서로 다른 개인정보처리자 간의 가명정보 결합을 수행하기 위해서는 개인정보보호위원회 또는 관계 중앙행정기관의 장이 지정하는 전문기관이 결합을 수행해서 배포해야 한다. 이 역할을 수행하는 기관을 '결합전문기관'이라고 한다.[6] 본 논문에서는 이러한 이유로 중앙에 '군 데이터 결합전문기관' 설치를 제안하였다.

2.3 결합키

개인정보보호위원회에서 발간한 '가명정보 처리 가이드라인'에서는 결합키를 '결합 대상 가명정보의 일부로서 해당 정보만으로는 특정 개인을 알아볼 수 없으나 다른 결합대상정보와 구별할 수 있도록 조치한 정보로서, 서로 다른 가명정보를 결합할 때 매개체로 이용되는 값'으로 정의하고 있다.[6] 서로 다른 정보들이 결합될 때 연계정보로 활용되고 최종 배포할 때는 삭제된다. '가명정보 처리 가이드라인'에서는 이 역할을 한국인터넷진흥원 또는 개인정보보호위원회가 지정하여 고시하는 기관이라고 설명하고 '결합키관리기관'이라고 명명하였다. 본 논문에서는 군 데이터를 처리하는 특수성을 감안하여 유사한 역할을 수행하는 '군 데이터 결합키관리기관'을 제안한다.

그림 1. 가명처리 프로세스

Fig. 1. Pseudonymization information process

그림 2. 가명정보 결합 프로세스

Fig. 2. Pseudonymous information combination process

2.4 가명처리 프로세스

'가명정보 처리 가이드라인' 에서는 가명처리에 대한 프로세스를 그림 1과 같이 제시하고 있다. 또한 가명정보 결합에 대한 프로세스도 그림 2와 같이 제시하고 있다.[6] 결합이 필요 없는 하나의 데이터 가명처리는 훈련장비에 권한이 있는 운용자 또는 조직 내 다른 인원이 자체적으로 가명처리하면 되지만 서로 다른 훈련장비 데이터 결합이 필요한 경우 결합전문기관과 결합키관리기관의 참여가 필요하다. 인공지능 등 통계 및 과학기술에 사용할 데이터는 입력되는 데이터의 범위가 넓을수록 정확한 결과를 도출해 낼 수 있다. 따라서 단일 데이터에 대한 가명처리 보다는 여러 데이터를 결합하여 질이 높은 데이터를 활용하기 위해 결합 프로세스는 빈번하게 이뤄져야 한다.

하지만 일반적인 민간 환경과 군 환경은 다르다. 훈련 데이터 사용을 원하는 조직 혹은 부대는 어떤 데이터가 언제 어떻게 생성되는지 알기 힘든 환경이다. 3장에서는 특수한 군 환경에 데이터 관리와 인공지능 기술을 접목하는 최근 연구들을 조사하여 소개한다.

3. 관련 연구

3.1 국방 분야 데이터 관리

앞서 언급한 바와 같이 군은 일반적인 환경과 다르다. 훈련장비 운용자는 군이라는 특수한 조직에 소속돼 있고 산출된 데이터는 다른 부대에서 어떤 종류의 데이터가 생성되는지 알 수 없어 이용하기 힘들다. 또한 산출되는 데이터의 종류를 파악한다고 해도 타 부대에 소속된 군이 데이터를 가져가기에는 협조가 어렵다. Kim et al.[7]은 이러한 군 환경에서 데이터를 전략적으로 활용할 수 있는 발전 방향을 단계별로 제시했다. 데이터 분석 및 융합을 위한 정보 요구 시 특별한 사유가 없는 한 데이터 제공을 의무화하고, 민감한 개인정보·군사정보 및 비밀 데이터 등은 안전한 활용을 위한 데이터 제공 및 활용 절차(기준)를 마련해야 한다고 제안하였다. Kim et al.[8]은 데이터가 모든 산업의 발전과 새로운 가치 창출의 촉매 역할을 하고 있고 스마트 국방혁신 추진사업과 군 및 범정부에서 추진하는 데이터 플랫폼 추진 사업을 데이터 가치사슬 측면에서 비교분석하고 국방데이터 생태계 구축을 위한 정책적 대안을 제시하였다. 또한 Park et al.[9]은 국방데이터책임관 제도 운영 현황을 점검해보고 다섯 가지 발전 방향을 제시했다. 이처럼 모든 산업에 데이터 활용이 증가됨에 따라 군도 데이터 수집과 활용에 대한 중요성을 인지하고 데이터 관리를 효과적으로 할 수 있는 발전적인 연구 방향을 제시하고 있다. 하지만 수집한 군 데이터를 과학기술 분야에 활용할 때 유출을 막을 수 있는 구체적인 방안을 제시한 연구 결과는 찾기 어렵다. 나아가 본 논문에서 제시한 방법과 같이 가명처리를 이용한 연구 결과는 현재 찾을 수 없다.

3.2 국방 분야 인공지능 기술 접목

방위사업청과 국방기술진흥연구소는 ``23~`37 국방기술기획서'을 출간하면서 인공지능 기술을 국방전략기술 10대 분야

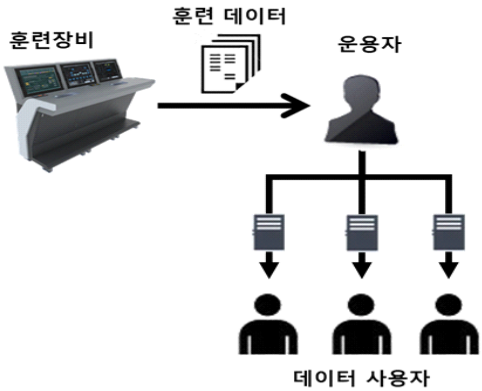

그림 3. 국방 교육훈련 데이터 관리 (현재 방식)
Fig. 3. Defense training data management (current method)

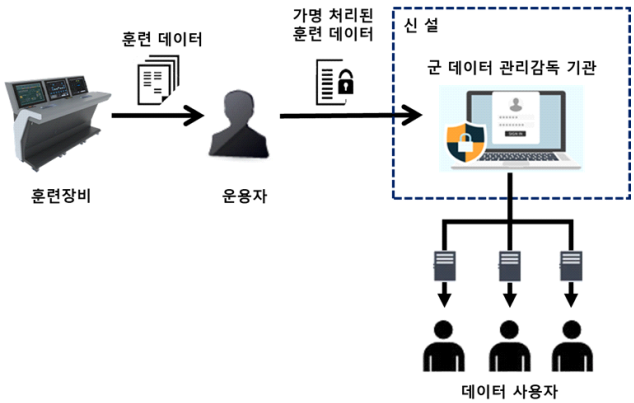

그림 4. 국방 교육훈련 데이터 관리 (제안 방식)
Fig. 4. Defense training data management (proposal method)

중 1순위로 포함시켰다. 이 문서에는 인공지능 분야 국방기술 44개 항목을 설명하고 이에 대한 중장기 계획을 포함하고 있다.[10] 이에 따라 현재 국방 분야에 인공지능 기술을 접목한 연구도 폭발적으로 나오고 있는 추세이다.

Yoon et al.[11]은 국방 인공지능 기술 업무에 종사하고 있는 50명을 대상으로 설문조사를 수행하였고 인공지능을 국방에 적용하는데 주요 시사점을 도출하였다. 설문조사 결과 총 11개의 분야 중 교육훈련 분야는 기술 활용도 측면에서 감시정찰 분야에 이어 2등에 위치했고, 1-5년 내 활용 가능한 측면에서도 국방정보시스템 분야에 이어 2등에 위치했다. 결론적으로 교육훈련 분야는 인공지능 기술 도입 시 기대 효과도 높을 뿐더러 윤리적 충돌 문제가 낮아 비교적 빠르게 인공지능 기술이 적용될 것으로 평가하였다.

본 논문에서는 현재 국방에서 가장 주목받는 기술인 인공지능 기술을 위한 효과적인 데이터 관리와 무분별한 데이터 사용으로 인한 유출을 방지하고자 데이터 가명처리 방안을 제안한다. 또한 많은 국방 분야 중 도입 시 기대효과가 높은 교육훈련 분야를 선정하여 그 범위를 줄였다.

4. 국방 교육훈련 데이터 가명정보 처리 방안

기존 국방 분야에서 훈련장비를 통해 산출되는 교육훈련 데이터는 운용자 및 관리자가 훈련장비로부터 데이터를 추출하여 개인별로 보관하고 있다가 필요로 하는 3자에게 직접 배포해주는 방식으로 진행되었다. 그림 3.은 현재 데이터 배포 방식을 보여준다.

본 논문에서 제안하는 교육훈련 데이터 배포 방식은 중앙에 모든 데이터를 관리·감독하는 조직을 신설하고 훈련 데이터의 이용을 원하는 사용자에게 관리·감독 조직이 데이터를 배포하는 형태이다. 또한 교육 훈련 장비의 데이터에는 운용자의 개인정보가 포함되어 있기 때문에 유출되어서는 안 된다. 따라서 교육 훈련 장비 운용자는 중앙 관리·감독 조직으로 데이터를 제공하기 전에 중요 정보를 필수적으로 가명처리 해야 함을 제안하였다. 이러한 이유로 본 논문에서는 중앙 관리·감독 조직으로 데이터를 보내기 전 훈련장비 운용자로부터 중요 정보는 가명처리하도록 제안하였다. 정리하자면 모든 교육훈련 데이터의 중요 정보는 가명처리된 후 관리·감독 조직이 수집하고 이를 필요로 하는 제 3자의 데이터 사용자에게 배포하는 것이다. 본 논문에서는 이 관리·감독 조직을 '군 데이터 관리·감독 기관'이라 명명하였다. 또한 교육훈련 데이터 가명처리 시 서로 다른 조직에서 산출된 데이터를 결합해야할 경우가 빈번히 발생될 것이다. '가명정보 처리 가이드라인'에서 '결합전문기관'과 '결합키관리기관'을 별도로 분리하고 데이터 결합 시 각 역할을 수행했던 것처럼 본 논문에서도 데이터 결합 시 '군 데이터 결합전문기관'과 '군 데이터 결합키관리기관'을 별도로 구성하였다. 그림 4.와 그림 5.는 본 논문에서 제안하는 훈련 데이터 관리 및 배포 방식을 보여준다.

훈련장비로부터 산출되는 훈련 데이터는 체계적으로 관리돼야 한다. 이를 위해 훈련장비 발주자인 군은 개발을 위한 요구사항부터 보호할 데이터를 식별하고 개발 업체에 발주해야 한다. 훈련장비 개발 업체는 요구사항 분석 단계부터 운용자의 개인정보로 보호될 항목과 민감한 데이터 항목을 식별해야 하고 개발단계에 산출되는 기술문서에 이를 기록해야 한다. 데이터 보호 측면에서 가명처리 대상 데이터 식별은 또 다른 기술이 접목돼야하므로 본 논문에서 다루진 않는다. 개발 완료 후 운용 단계에 산출되는 훈련 데이터들은 '군 데이터 관리·감독 기관'이 기술문서로부터 어떤 데이터들이 산출되는지 파악할 수 있다. 여기서 '군 데이터 관리·감독 기관'이 확인할 수 있는 데이터는 데이터의 종류만 확인할 수 있을 뿐이지 실제 데이터까지 공유해서는 안 된다. 실제 운용 단계에서 산출된 훈련 데이터는 훈련장비 운용자로부터 가명처리되고 '군 데이터 관리·감독 기관'으로 전달되어 관리돼야 한다. 즉, '군 데이터 관리·감독 기관'은 '최소 권한의 원칙'에 따라 훈련 데이터에 대한 종류는 파악할 수 있으나 실제 데이터에 대한 열람 권한은 가져서는 안 된다.

본 논문이 제안하는 방안에서는 '군 데이터 관리·감독 기관'의 역할이 중요하다. 첫 번째로 '군 데이터 관리·감독 기관'은 군에서 사용되는 훈련장비 목록을 범주화 하고 주기적으로 데이터를 수집해야 한다. 인공지능, 빅데이터 등 현재 주목받는 기술들은 데이터의 양이 성패를 가르기 때문에 그 역할은 매우 중요하다. 두 번째로 수집된 데이터의 위험성을 검토할 역할을 수행해야 한다. 가명처리된 데이터를 받았다고 하더라도 추가적으로 가명처리할 데이터는 없는지 가명처리 적정성을 검토하고 외부에 공개돼서는 안 되는 데이터는 없는지 등 데이터에 대한 위험성 검토가 이뤄져야 한다. 세 번째로 데이터 결합 시 데이터 결합률과 모의결합에 대한 정보를 공유할 수 있어야 한다. 마지막으로 '군 데이터 관리·감독 기관'은 어떤 무기체계의 훈련 데이터인지, 훈련 데이터가 제공하는 항목은 무엇이 있는지 등을 데이터 사용자들에게 홍보할 필요가 있다. 이를 위해 데이터 사용자들에게 설명 자료가 공유될 수 있도록 자료화해야 한다.

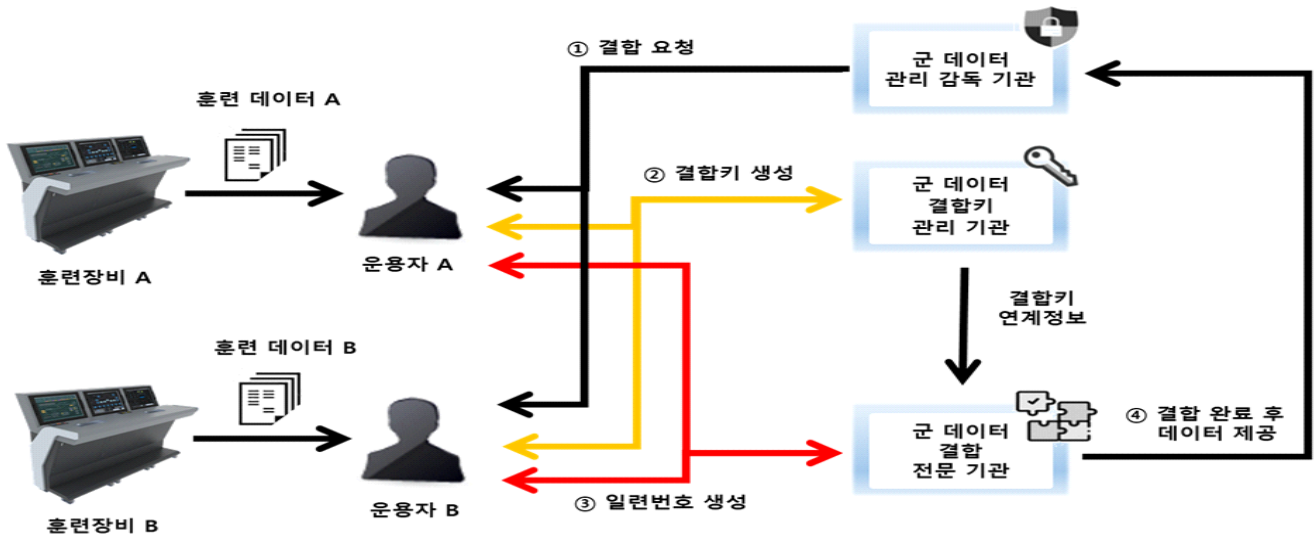

그림 5. 국방 교육훈련 데이터 결합 절차
Fig. 5. Defense training data combination procedure

그림 1.에서 제시한 바와 같이 가명처리 세부절차는 ① 목적 설정 등 사전준비, ② 위험성 검토, ③ 가명처리, ④ 적정성 검토, ⑤ 안전한 관리 순으로 5단계에 걸쳐서 진행된다. 본 논문에서는 이 5단계에 따라 교육훈련 데이터 관리 방안에 대해 제안한다. 또한 그림 2.의 가명정보 결합 절차를 참고하여 본 논문에서 제시하는 가명정보 결합 방안에 대해서도 설명한다.

4.1 목적 설정 등 사전준비

데이터 사용자는 데이터를 필요로 하는 분명한 목적을 가지고 '군 데이터 관리·감독 기관'이 배포하는 훈련 데이터 설명 자료를 검토한다. 그러기 위해선 명확한 사업 목적과 원하는 데이터 항목이 무엇인지 충분히 검토해야 한다. 사전 준비된 자료를 가지고 '군 데이터 관리·감독 기관'과 협의하여 데이터를 습득할 날짜, 사용 기간, 폐기 날짜 등을 확정한다.

4.2 위험성 검토

훈련장비 운용자의 개인정보 및 중요 정보가 가명처리 되었다고 해도 향후 악용될 가능성은 다양한 측면에서 검토해야 한다. 특히 군 정보는 국가 안보와 직결된 정보이다. 위협은 외부 공격자뿐만 아니라 내부자도 고려해야 한다. 따라서 정보의 노출은 최소화하고 보안 전문가의 검토가 가장 중요한 단계이다. 데이터에 문제가 없는지, 데이터를 처리하는 환경에는 문제가 없는지 등 복합적인 방법으로 위험성을 검토한다. 또한 '군 데이터 관리·감독 기관'은 가명처리된 데이터 외 추가로 가명처리해야 할 데이터는 없는지 검토 후 훈련장비 운용자에게 알려줘야 한다.

4.3 가명처리

'가명정보 처리 가이드라인'에서는 데이터 사용자가 데이터를 요청할 때 가명처리가 이뤄지지만 본 논문의 개념은 다르다. 본 논문에서는 훈련장비로부터 훈련 데이터가 나오면 운용자가 가명처리하고 '군 데이터 관리·감독 기관'에 전달된다. '군 데이터 관리·감독 기관'은 이미 가명처리된 데이터를 가지고 있는 상태에서 데이터 사용자로부터 사용 요청을 받는다. 다만 그림 2.와 같이 서로 다른 데이터와 결합이 필요한 경우가 있다. 가명정보 결합에 대한 내용은 4.6절에서 제시한다.

4.4 적정성 검토

'군 데이터 관리·감독 기관'은 데이터 사용자에게 배포 전 적정성을 검토하고 추가 보호할 데이터 항목이 있다면 훈련장비 운용자에게 요청하여 추가 가명처리된 데이터를 받는다. 이때 다른 정보와 결합을 통해 개인정보가 노출될 수 있는지, 연구에 필요한 데이터가 가명처리로 인해 부족해지지 않았는지 등을 검토하여 적정성을 검토한다.

4.5 안전한 관리

데이터 사용자에게 가명처리된 데이터를 배포하고 다른 목적으로 사용되지 않도록 관리한다. 파기 일자를 정해둬 추후 보안감사 시 확인할 수 있다. 다른 추가 정보로 인해 민감한 정보가 노출되지 않도록 주기적인 관리가 이뤄져야 한다.

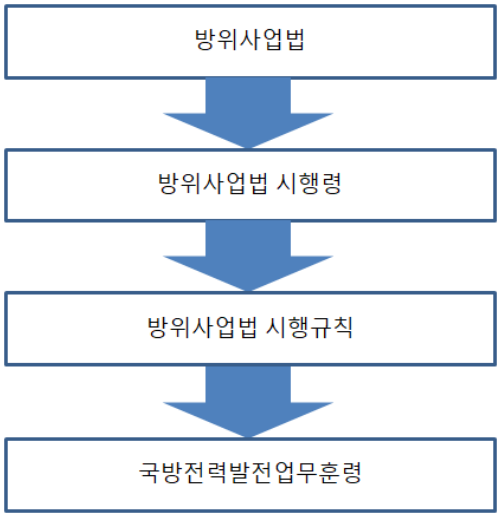

그림 6. 국방전력발전업무훈령 법률 체계
Fig. 6. Legal system diagram of the 'Defense Force Development Work' Directive

4.6 가명정보 결합

2개 이상의 훈련장비로부터 산출된 훈련 데이터를 결합할 때는 그림 2.와 같이 결합 절차를 지켜야 한다. 본 논문에서 제시하는 결합 절차를 구조화한 결과가 그림 5.이다. '가명정보 처리 가이드라인'과 크게 다르지 않지만 본 논문에서는 '군 데이터 관리·감독 기관'이 주관하고 통제하도록 제안하였다. 서로 다른 훈련 데이터를 결합하려면 결합키와 일련번호 생성이 필요하다. '군 데이터 관리·감독 기관'이 가지고 있는 데이터는 가명처리된 데이터기 때문에 결합 기준을 알 수 없다. 이러한 이유로 '군 데이터 관리·감독 기관'은 훈련 데이터 처리 권한이 있는 운용자에게 결합키 생성과 일련번호 생성을 요청해야 한다. 이때 지원하는 기관이 '군 데이터 결합키관리기관'과 '군 데이터 결합전문기관'이다. '가명정보 처리 가이드라인'에서는 이미 데이터 열람 권한이 없는 사람을 배제하고 데이터를 결합할 수 있는 방법을 자세하게 가이드하고 있다. 그림 5.에서 결합키 생성과 일련번호 생성 및 데이터 결합은 '가명정보 처리 가이드라인'과 동일한 방법으로 진행한다.

5. 법체계 정합성을 위한 제언

제안한 교육훈련 데이터 가명처리를 위해 현재 군에서 관련 있는 법률을 파악하고 부족한 부분을 채울 수 있도록 법률체계 개정을 제안한다.

5.1 국방 개인정보보호 훈령

'국방 개인정보보호 훈령'[12]은 국방부 소관 분야의 개인정보보호에 필요한 세부적인 사항을 규정하는 국방 분야의 행정규칙이다. 그러나 일반적인 내용만 제시되어 있을 뿐 교육훈련과 관련된 데이터를 취급하거나 인공지능, 빅데이터 등 연구 분야에서 사용되는 데이터에 대한 고려사항은 언급되지 않았다. 무엇보다 현재 시행중인 '국방 개인정보보호 훈령'은 데이터 3법이 개정된 2020년도보다 이전인 2019년도에 개정된 버전으로

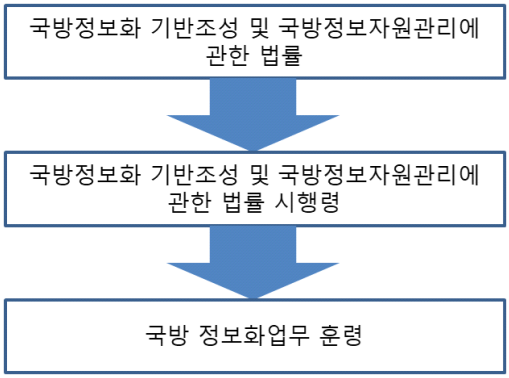

그림 7. '국방 정보화업무 훈령' 법률 체계
Fig. 7. Legal system diagram of the 'Defense Information Work' Directive

개인정보보호와 관련된 내용이 상세하게 풀려 있지 않고 현재까지도 개정되고 있지 않다.

5.2 국방 전력발전업무 훈령

국방전력발전업무훈령[13]은 군과 방위사업에 관련된 전 기관을 대상으로 군수품 획득과 운영 및 유지에 관한 지침을 제공하는 규정이다. 즉, 무기체계 교육훈련장비 개발업체와 획득 및 운용 조직인 군과 관련된 훈령이다. 이 훈령 또한 운용자의 개인정보와 훈련장비로부터 산출되는 데이터 관리에 대해 언급되고 있지 않다. 데이터 중심의 국방 환경을 구축하기 위해선 국방전력발전업무훈령에서 데이터에 대한 운용 및 관리 기준이 제시되어야 한다. 또한 교육훈련장비 운용자들이 데이터를 가명처리하기 위해선 국방전력발전업무훈령에 데이터 보호에 대한 가명처리 규정이 반영되어 개정돼야 한다. 국방전력발전업무훈령의 법률 체계는 그림 6.과 같다.

5.3 국방 정보화업무 훈령

'국방 정보화업무 훈령'[14]은 국방 정보시스템을 운용함에 있어 운용 및 관리를 위한 훈령이다. 무기체계 운용자 관점에서 준수해야하는 훈령이다. '국방 정보화업무 훈령'은 '국방 정보화기반조성 및 국방정보지원관리에 관한 법률'로부터 '국방 정보화기반조성 및 국방정보자원관리에 관한 법률 시행령'으로 상위 법률이 구성되어 있다. '국방 정보화기반조성 및 국방정보자원관리에 관한 법률'에서는 국방통합데이터센터령과 연관을 짓는데 국방통합데이터센터령은 컴퓨터 체계에 대한 관리 및 운영 업무를 국방부 장관 소속인 국방통합데이터센터에서 관장하도록 구성되어 있다. 자세한 구조도는 그림 7.를 참고한다.

5.4 국방통합데이터센터령

국방통합데이터센터령[15]은 국방정보시스템 중 컴퓨터체계에 대한 관리 및 운영 업무를 통합하여 관장하기 위한 훈령이다. 관리 대상이 되는 컴퓨터체계 중 군사정보 및 개인정보 보호 등을 고려하여 국방부 장관이 정하는 컴퓨터체계는 제외하고 있다. 해당 훈령은 조직의 구성과 목적만 기술돼 있고 세부 수행 지침 내용은 찾을 수 없다. 데이터 중심의 군 환경을 만들고자 한다면 국방통합데이터센터의 역할을 세분화하고 교육훈련장비에서 생성되는 데이터도 관리 대상으로 포함시켜야 한다.

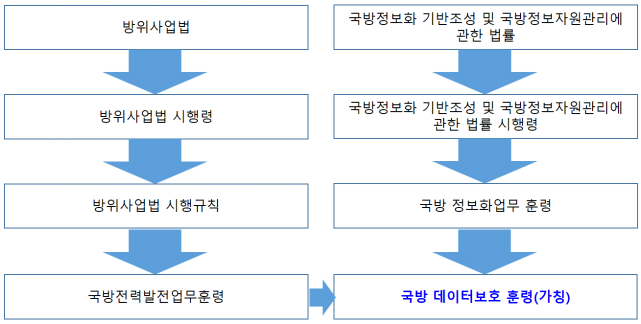

그림 8. '국방 데이터보호 훈령' 제정 제안
Fig. 8. Proposal to enact the 'Defense Data Protection' Directive

5.5 훈령 개정 제언

기존 국방전력발전업무훈령과 '국방 정보화업무 훈령'에는 개인정보 또는 훈련장비로부터 산출되는 민감한 정보를 보호하는 규정이 없어 주의가 불필요했을지도 모른다. 인공지능 등 첨단 기술이 도입 되면서 많은 교육훈련 데이터가 점차 공유될 것으로 예측되고 있다. 공유되는 데이터 보호를 위해 본 논문에서 제시하는 가명처리를 포함하여 데이터 보안을 위한 법률이 갖춰져 있어야 한다. 따라서 교육훈련장비 개발 및 획득 과정에서 적용되는 국방전력발전업무훈령과 운용 과정에서 적용되는 '국방 정보화업무 훈령'을 그림 8.과 같이 '국방 데이터보호 훈령(가칭)'을 가리키도록 개정해야 한다.

6. 기대효과 및 향후연구

본 논문에서는 중앙에 교육훈련 데이터를 관리하는 '군 데이터 관리·감독 기관'을 두었지만 그 목적에 따라 이를 다른 방향으로 적용할 수도 있다. 예를 들어 '군 데이터 관리·감독 기관'이 일반 장병들을 대상으로 여러 가지 훈련 방법에 대한 성취도를 분석하기 위한 데이터를 관리하는 역할을 수행한다면 본 논문이 제안하는 데이터 정보보호 메커니즘을 그대로 가져갈 수 있다. 그러나 현재 논문에서는 제안하는 방법론을 입증할 데이터는 제공하지 못했다. 향후 연구로는 제안하는 방법론을 입증을 위한 실제 가명처리 사례를 통해 방법론을 보강할 예정이다.

현 방위산업 구조상 훈련장비를 개발하는데 있어 수많은 협력업체가 동원된다. 이 과정에서 현재까지는 데이터 유출로 인한 개인정보보호에 안일하게 대처했었다. 제안된 무기체계 훈련장비 데이터를 국방통합데이터센터로부터 홍보되고 데이터 관리 감독 기관으로부터 가명처리 프로세스대로 배포된다면 데이터를 사용한 인원과 그 목적이 관리되기 때문에 내부자 보안 취약점을 통해 운용자의 개인 정보가 유출되는 사고를 막을 수 있다. 추후 이를 발전시켜 군 환경에서 개인정보보호

를 강화하는데 관련 규정과 범위를 더 확장시키는 연구가 필요하다.

References

[1] Korean Ministry of National Defense(MND), “Defense Data Analysis Center, an organization specialized in defense data, opened”, Korea Policy Briefing, 2023.01, https://www.korea.kr/briefing/pressReleaseView.do?newsId=156549970

[2] Youngmook Kim, “Development and application of artificial intelligence for military training modeling and simulation in Republic of Korea”, Journal of Advances in Military Studies, Vol. 4, No. 2, pp. 21-36, 2021

[3] Jung-Ho Eom, Nam-uk Kim, “Measures to Prevent the Leakage of Military Internal Information through the Analysis of Military Secret Leakage Cases: Focusing on Insider Behaviors”, Journal of convergence security, Vol. 20, No. 1, pp. 85-92, 2020

[4] Yun-Hee Kim, “Increased threat of hacking that neutralizes even network partitioned networks”, 2021, Retrieved from https://zdnet.co.kr/view/?no=20191216132608

[5] Personal Information Protection Commission, “PERSONAL INFORMATION PROTECTION ACT”, ACT No. 16930, February 4, 2020

[6] Personal Information Protection Commission, “Pseudonymization Guideline”, Feb. 2020

[7] Seyonh Kim, Junsang Kim, Seokwon Kang, “A Study on the Strategic Application of National Defense Data for the Construction of Smart Forces in the 4th IR” Journal of convergence security, Vol. 20, No. 4, pp.113-123, 2020

[8] Sungtae Kim, “Development Direction of Building Defense Data Ecosystem”, Journal of the Korea Institute of information and communication engineering, Vol. 26, No. 1, 2022

[9] Taehyun Park, Sungtae Kim, “An Improvement Strategy on the Chief Data Officer of MND”, Journal of the Korea Institute of information and communication engineering, Vol. 26, No. 1, 2022

[10] Defense Acquisition Program Administration(DAPA), “’23-’27 Defense Technology Planning”, DAPA, pp. 1-335, 2023

[11] Junghyun Yoon. “Major Issues in the introduction of AI Technology in the Defense Field and Plans to Improve Utilization”, SCIENCE & TECHNOLOGY POLICY(STEPI) Insight, Vol. 279, pp. 1-55, 2021

[12] Korea Ministry of National Defense(MND), “Defense Personal Information Protection Directive”, MND Directive No. 2328, October 14, 2019

[13] Korea Ministry of National Defense(MND), “Defense Force Development Operation Directive”, MND Directive No. 2568, June 30, 2021

[14] Korea Ministry of National Defense(MND), “Defense Informatization Task Directive”, MND Directive No. 2436, June 4, 2021

[15] Korea Ministry of National Defense(MND), “Defense Integrated Data Center Decree”, Presidential Decree, No. 28475, December 9, 2017