



제 439회 국회 (정기회)
제1차 과학기술정보방송통신위원회

전기통신사업법 일부개정법률안

검 토 보 고

〈메신저 서비스 이용 범죄 예방을 위한 기술적·관리적 조치 규정〉
■ 허성무의원 대표발의(의안번호 제2217820호)

2026. 9.

과학기술정보방송통신위원회

수석전문위원 이지민

목 차

I . 제안경 위	1
II . 제안이유 및 주요내용	1
III . 검토의견	2
1. 메신저 서비스 이용 범죄 예방을 위한 기술적·관리적 조치 규정	2

I. 제안경위

가. 발 의 자 : 허성무의원 등 10인

나. 발의연월일 : 2026. 3. 27.

다. 회부연월일 : 2026. 3. 30.

II. 제안이유 및 주요내용

현행법은 전기통신사업의 건전한 발전과 이용자의 편의를 도모함으로써 공공복리의 증진에 이바지하는 것을 목적으로 하고, 전기통신사업자가 그 업무를 처리할 때 공평하고 신속하며 정확하게 하도록 규정하고 있음.

그러나 전화번호 등 이용자 식별정보를 연계하여 제공되는 메신저 서비스가 보편적인 의사소통 수단으로 활용됨에 따라 이를 이용한 사기 등 범죄로 인한 이용자 피해가 지속적으로 발생하고 있음에도, 메신저 서비스의 이용 과정에서 범죄를 예방하기 위한 기술적·관리적 조치에 관하여는 명확한 규정이 마련되어 있지 않음.

이에 메신저 서비스를 제공하는 부가통신사업자에게 이용자의 접속 국가가 다른 경우 이를 표시하도록 하는 등 필요한 기술적 조치를 하도록 하고, 범죄 관련 의심 계정에 대한 상시 신고 기능을 마련하도록 하며, 신고를 받은 경우 지체 없이 필요한 조치를 하도록 하려는 것임 (안 제84조의3 신설 등).

Ⅲ. 검토의견

1. 메신저 서비스 이용 범죄 예방을 위한 기술적·관리적 조치 규정

가. 개정안의 내용

- 개정안은 문자·음성을 이용하여 사람과 대화하는 방식으로 정보를 처리하는 시스템을 기반으로 하는 부가통신역무(이하 “메신저서비스”라 함)를 제공하는 자(이하 “메신저서비스 제공자”라 함)에게 메신저서비스 이용 범죄 예방을 위하여 ① 이용자의 메신저서비스 가입 시와 이용 시의 접속국가가 다를 경우 이를 표시하기 위한 기술적 조치, ② 범죄 관련 의심계정 신고를 위한 상시 신고체계 구축 등 기술적·관리적 조치를 하도록 하고, 신고를 받으면 지체없이 계정 정지등 필요한 조치 후 신고자 및 이용자에게 그 사실을 알릴 의무를 부과하며, 위반 시 5천만원 이하의 과태료를 부과하려는 것임(안 제84조의3 및 제104조 제1항제6의2·제6의3 신설).

현 행	개 정 안
<신 설>	제84조의3(메신저 서비스의 범죄 예방을 위한 기술적·관리적 조치 등) ① 제22조제1항에 따라 부가통신사업을 신고한 자 중 문자·음성을 이용하여 사람과 대화하는

현행	개정안
	방식으로 정보를 처리하는 시스템을 기반으로 하는 부가통신역무(이하 “메신저서비스”라 한다)를 제공하는 자(이하 “메신저서비스 제공자”라 한다)는 메신저서비스를 이용한 범죄를 예방하기 위하여 다음 각 호의 기술적·관리적 조치를 하여야 한다. 1. 이용자의 메신저서비스 가입 시 접속 국가와 메신저서비스 이용 시 접속 국가가 다를 경우 이를 표시하기 위한 기술적 조치 2. 메신저서비스를 이용한 범죄 관련 의심 계정(메신저서비스 제공자가 이용자를 식별·관리하기 위하여 사용하는 이용권한 계좌를 말한다. 이하 같다) 신고를 위한 상시 신고 체계 구축 ② 제1항제2호에 따른 신고를 받은 메신저서비스 제공자는 지체 없이 계정 정지 등 필요한 조치를 하여야 하고 신고한 자 및 해당 계정 이용자에게 그 사실을 알려야 한다. ③ 제1항에 따른 기술적·관리적 조치, 제2항에 따른 필요한 조치

현행	개정안
제104조(과태료) ① 다음 각 호의 어느 하나에 해당하는 자에게는 5천만원 이하의 과태료를 부과한다. 1. ~ 6. (생략) <u><신설></u> <u><신설></u> 7. (생략) ② ~ ⑥ (생략)	<u>의 방법·절차 등에 필요한 사항은 대통령령으로 정한다.</u> 제104조(과태료) ① ----- ----- ----- -----. 1. ~ 6. (현행과 같음) <u>6의2. 제84조의3제1항을 위반하여</u> <u>각 호에 따른 조치를 하지 아니한 자</u> <u>6의3. 제84조의3제2항을 위반하여</u> <u>필요한 조치를 하지 아니한 자</u> 7. (현행과 같음) ② ~ ⑥ (현행과 같음)
부칙	
이 법은 공포 후 6개월이 경과한 날부터 시행한다.	

나. 검토의견

- 최근 전화번호 등 이용자 식별정보를 연계한 메신저서비스가 주된 의사소통 수단으로 자리 잡으면서, 이를 매개로 하는 메신저 피싱, 투자사기 등 범죄의 고도화가 지속되고 있음.
- 특히, 해외접속 IP를 이용하여 국내 가입자인 것처럼 속이거나, 대포 계정을 활용한 범죄가 지속적으로 발생함에 따라 이용자 피해 역시 심각한 수준으로 발전하고 있음.

- 경찰청 조사결과에 따르면, 전기통신서비스를 이용한 금융사기 행위 중 메신저서비스를 이용한 피싱이 2024년에는 5,809건, 2025년에는 5,049건 발생하였고, 피해액도 각각 322억원, 250억원에 이르고 있음.
- 또한, 투자리딩방, 로맨스스캠, 노쇼사기 등 주로 메신저서비스(SNS)를 통해 발생하는 다중피해사기의 경우 2025년에 총 19,973건의 사기행위를 통해 1조 593억원의 피해액이 발생하여, 2024년 총 9,369건의 사기행위를 통해 7,779억원의 피해가 발생한 것에 비해 피해 규모가 큰 폭으로 증가하고 있는 것으로 나타남.

<전기통신금융사기 및 다중피해사기 피해 현황>

구분	계	전기통신금융사기						다중피해사기				
		소계	보이스 피싱	메신저 피싱	투자리딩방	로맨스 스캠	노쇼사기	소계	투자리딩방	로맨스 스캠	노쇼사기	팀미션
발생건수(건)	'24년	42,565	33,196	20,839	5,809	2,152	4,396	9,369	8,104	1,265	-	-
	'25년	52,265	32,292	23,360	5,049	1,198	2,685	19,973	6,853	2,192	6,515	4,413
피해액(억원)	'24년	17,108	9,329	8,545	322	112	546	7,779	7,104	675	-	-
	'25년	23,755	13,162	12,578	250	70	328	10,593	6,581	1,360	1,256	1,396

자료: 경찰청, 공공데이터포털

- 이러한 상황을 감안하여 메신저서비스를 활용한 사기범죄를 예방할 수 있는 법적·제도적 기반을 강화할 필요성이 있다는

지적이 지속적으로 제기되고 있음¹⁾.

- 그런데, 현행법은 보이스피싱 범죄를 예방하기 위한 방안으로 전화번호의 거짓표시를 금지하고, 전기통신사업자에게 거짓 전화번호 표시를 차단하는 조치를 하여야 할 의무를 부여²⁾하고 있으나, 웹이나 앱 기반의 부가통신역무인 메신저서비스를 이용한 사기범죄의 예방을 위한 조치나 의심 계정의 제재와 관련한 명확한 의무규정은 미비한 실정임.

-
- 1) 2026. 5. 27. 이데일리, “7개월 연속 감소”...정부, 보이스피싱 꺾었지만 SNS 기반 신종 사기 확산에 긴장(<https://www.edaily.co.kr/News/Read?newsId=0523488645453184&mediaCodeNo=257&OutLnkChk=Y>)
- 2) 「전기통신사업법」 제84조의2(전화번호의 거짓표시 금지 및 이용자 보호) ① 누구든지 다른 사람을 속여 재산상 이익을 취하거나 폭언·협박·희롱 등의 위해를 입힐 목적으로 전화(문자메시지를 포함한다. 이하 이 조에서 같다)를 하면서 송신인의 전화번호를 변작하는 등 거짓으로 표시하여서는 아니 된다.
- ② 누구든지 영리를 목적으로 송신인의 전화번호를 변작하는 등 거짓으로 표시할 수 있는 서비스를 제공하거나 송신인의 전화번호를 변작하는 등 거짓으로 표시할 수 있는 장치를 제조, 수입, 배포, 판매, 대여하여서는 아니 된다. 다만, 공익을 목적으로 하거나 수신인에게 편의를 제공하는 등 정당한 사유가 있는 경우에는 그러하지 아니하다.
- ③ 전기통신사업자는 거짓으로 표시된 전화번호로 인한 이용자의 피해를 예방하기 위하여 다음 각 호의 조치를 하여야 한다. 다만, 제2항 단서에 따른 정당한 사유가 있는 경우는 제외한다.
1. 변작 등 거짓으로 표시된 전화번호의 전화 발신을 차단하거나 송신인의 정상적인 전화번호로 정정하여 수신인에게 송출하기 위한 조치
2. 국외에서 국내로 발신된 전화에 대한 국외발신 안내를 위한 조치
3. 변작 등 거짓으로 표시한 전화번호를 송신한 자의 해당 회선에 대한 전기통신역무 제공의 중지를 위한 조치
4. 그 밖에 이용자 보호를 위하여 과학기술정보통신부장관이 정하는 사항
- ④ 과학기술정보통신부장관은 제3항에 따른 조치의 이행 여부를 확인하거나 이용자의 피해가 확산되는 것을 방지하기 위하여 전기통신사업자에게 다음 각 호에 해당하는 자료의 열람·제출을 요청하거나 필요한 검사를 할 수 있다.
1. 변작 등 거짓으로 표시된 전화번호의 전화 발신을 차단한 경우 해당 전화번호, 차단시각, 발신 사업자명
2. 수신자가 변작 등 거짓으로 표시된 전화번호에 대하여 신고한 경우 발신 사업자명
3. 그 밖에 제3항 각 호의 조치 이행 여부를 확인할 수 있는 관계 자료
- ⑤ 과학기술정보통신부장관은 제3항에 따른 조치의 이행 여부를 확인하고 제4항에 따른 조치를 시행하기 위하여 대통령령으로 정하는 바에 따라 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제52조에 따른 한국인터넷진흥원에 업무를 위탁하고 이에 소요되는 비용을 지원할 수 있다.
- ⑥ 과학기술정보통신부장관은 제2항 단서에 따른 정당한 사유, 제3항 각 호에 따른 조치 및 제4항의 이행을 위한 구체적인 절차·방법을 정하여 고시할 수 있다.
- ⑦ 제4항에 따른 자료의 열람·제출 및 검사에 대하여는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제64조, 제64조의2 및 제69조를 준용한다.

- 이에 개정안은 메신저서비스 제공자에 대하여 '이용자의 국가 간 접속 불일치 표시' 및 '범죄 의심 계정의 상시 신고 체계' 등의 기술적 조치 의무를 부여하고, 해당 의무 위반 시 5천만원 이하의 과태료를 부과하려는 것임.
- 개정안에 따르면, 해외에 거점을 두고 국내 메신저 계정을 도용하여 가족 또는 지인을 사칭하는 경우 가입 국가와 접속 국가의 상이함에 대한 경고 문구를 통해 기만행위를 사전에 인지함으로써 범죄 피해를 예방할 수 있을 것으로 기대되며, 의심계정 신고에 대해 사업자에게 직접적인 관리 책임을 부여함으로써 보다 신속한 조치도 가능할 것으로 보인다는 점에서, 개정안의 입법 취지는 긍정적인 측면이 있는 것으로 보임.
- 다만, 개정안과 관련하여서는 다음 사항을 검토할 필요가 있는 것으로 보임.
- 첫째, 메신저서비스 이용자의 관점에서 기본권 침해의 우려가 있는 것으로 보임.
- 개정안은 범죄 관련 의심 계정으로 신고된 계정에 대해 지체없이 정지 등 필요한 조치를 하도록 규정하고 있는데, 만약 악의적인 허위 신고나 오인 신고가 접수될 경우 정상적인 이용자의 계정이 사실 확인이나 별도의 소명 절차도 없이 즉시 정지되는 사례가 발생할 수 있음.

- 현대 사회에서 메신저의 계정 정지는 일상적·경제적 소통의 차단을 의미하는바, 선량한 피해자를 방지하기 위한 별도의 수단 없이 지체 없는 계정 정지 조치만을 규정할 경우 과잉 규제 논란이 제기될 수 있는 것으로 보임.
- 또한, 접속 국가의 불일치를 메신저에 표시할 경우 출장, 여행, 유학 등 범죄와 무관한 사유로 해외 체류 중인 이용자의 접속 국가가 본인의 의사와 무관하게 타인에게 공개되어 이용자의 사생활이 침해되는 문제가 발생할 우려도 있는 것으로 보임.
- 둘째, 개정안의 적용대상인 메신저서비스 사업자에는 카카오(카카오톡), 네이버(라인) 등 국내 사업자 뿐 아니라 텔레그램, 텐센트(위챗), 메타(페이스북메신저, 인스타그램DM, 왓츠앱) 등 다수의 해외사업자가 포함될 것으로 보이는데, 이러한 해외사업자에 대한 규범력 확보에 어려움이 있을 수 있다는 지적이 있음.
- 이와 관련하여 개정안의 소관 부처인 과학기술정보통신부는 본사가 해외에 있는 해외 사업자들에 대해 본국의 법령과 다른 규제를 적용할 경우 국가 간 통상 문제로 확대될 우려가 있고, 특히 텔레그램과 같이 국내에 서버나 법인을 두고 있지 않은 해외 메신저서비스 제공자에 대해서는 현실적으로 국내법의 적용을 강제하기가 어려운 측면이 있다는 점을 고려할 때, 개정안의 규범력은 결국 국내 메신저서비스 제공자에 대해서만

확보되어 국내 사업자를 역차별하는 결과로 이어질 우려가 있다는 의견을 제시하고 있음.

○ 셋째, 가입 국가와 이용 국가는 IP주소나 MCC(국가코드)³⁾를 통해 식별할 수 있는데, 만약 이용자가 VPN(가상 사설망)을 활용하여 국내 IP로 우회 접속할 경우 시스템상 접속 국가가 한국으로 동일하게 인식되므로, 개정안에 따른 기술적 조치가 무력화되어 규제의 실효성이 상실될 우려가 있음.

○ 넷째, 개정안의 입법취지를 달성하기 위해서는 메신저를 사용하는 모든 이용자의 가입 시 위치정보와 접속 IP의 국가 정보를 실시간으로 추적·비교하여야 하는바, 이 과정에서 다른 나라의 개인정보 관련 법령과 충돌할 우려가 있음.

- 예를 들어, EU의 「일반개인정보보호법」(GDPR) 제5조⁴⁾는 개인정보는 구체적이고 명시적이며 정당한 목적으로 수집되어야 하고, 그 목적을 달성하는데 필요한 범위로 한정(‘개인정보 최소화’)되어야 한다고 규정하고 있고, 같은 법 제6조⁵⁾는 개인정보의

3) Mobile Country Code: 이동통신에서 국가를 식별하는 3자리 코드

4) Art. 5 GDPR Principles relating to processing of personal data

1. Personal data shall be:

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes (‘purpose limitation’);

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);

5) Art. 6 GDPR Lawfulness of processing Processing shall be lawful only if and to the extent that at least one of the following applies:

1. Processing shall be lawful only if and to the extent that at least one of the following applies:

처리는 정보 주체가 하나 이상의 구체적 목적을 위한 처리에 동의한 경우이거나, 정보 관리자(개인정보처리자)에게 적용되는 법적 의무 준수를 위해 처리가 필요한 경우 등에 해당하는 경우에만 합법적이며, 그 의무의 법적 근거가 EU 법률이거나 개인정보처리자에게 적용되는 회원국(EU 가입국가) 법률에 해당하여야 한다고 규정하고 있음.

<접속국가 정보 수집에 관한 EU GDPR의 관련 규정>

제5조	1. 개인정보는 다음 각 호에 따라 처리되어야 한다. (b) 구체적이고 명시적이며 정당한 목적을 위하여 수집되어야 하며, 그 목적과 양립할 수 없는 방식으로 추가 처리되어서는 아니 된다. 다만, 공익을 위한 기록 보존, 과학적·역사적 연구 또는 통계 작성의 목적으로 제89조제1항에 따라 추가 처리하는 경우에는 당초의 목적과 양립할 수 없는 것으로 보지 아니한다(‘목적 제한’). (c) 처리 목적과 관련하여 적절하고 관련성이 있으며, 그 목적을 달성하는 데 필요한 범위로 한정되어야 한다(‘개인정보 최소화’).
제6조	1. 개인정보 처리는 다음 각 호 중 하나 이상에 해당하는 경우에 한하여, 그리고 그에 해당하는 범위에서만 적법하다. (a) 정보주체가 하나 이상의 구체적인 목적을 위하여 자신의 개인정보를 처리하는 데 동의한 경우 (c) 개인정보처리자에게 적용되는 법적 의무를 준수하기 위하여 처리가 필요한 경우 3. 제1항 (c) 및 (e)에 따른 개인정보 처리의 근거는 다음 각 호 중 하나의 법률로 정하여야 한다. (a) <u>유럽연합 법률</u> 또는 (b) <u>개인정보처리자에게 적용되는 회원국 법률</u>

자료: 과학기술정보통신부

- (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- (c) processing is necessary for compliance with a legal obligation to which the controller is subject;
3. The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by:
- (a) Union law; or
- (b) Member State law to which the controller is subject.

- 그런데, 개정안은 정보주체의 가입·접속 국가 정보 제공 동의에 관한 내용을 규정하지 않고 있으며, 우리나라 법률에 따른 법적 의무를 준수하는 메신저서비스 제공자는 EU GDPR에서 개인정보 처리를 허용하는 ‘개인정보처리자’에도 해당하지 않음.
- 따라서 개정안과 같이 이용자 접속국가의 표시를 의무화 하더라도 EU GDPR의 적용을 받는 이용자에 대해서는 입법 목적을 달성하는 데 한계가 있을 것으로 보임.

다. 정부 및 관련 단체 의견

1) 과학기술정보통신부: 신중검토

- 메신저를 이용한 피싱 등으로 인해 지속적으로 발생하고 있는 피해를 예방하기 위한 법적 근거가 필요하다는 입법취지에는 공감하나, ① 해외 사업자에 대한 규제 관할권 및 집행력 확보가 어려워 국내 사업자에 대한 역차별이 발생할 우려가 있고, ② 접속 국가를 구체적으로 노출되는 것에 거부감을 느끼는 이용자가 있을 것으로 예상되며, ③ 해외 각국의 개인정보 관련 법령과 충돌할 가능성이 있음.
- 또한, 현재 메타, 카카오 등 주요 메신저 사업자들이 가입 국가와 접속 국가를 단순 비교·표시하는 방식이 아닌 AI기반 이상행위 탐지 등 보다 정교하고 다양한 기술적 방식을 통해 피싱·사

칭에 대응하고 있다는 점을 고려할 때, 개정안과 같이 특정 기술 방식을 법령으로 일률적으로 강제하기보다는 각 사업자가 서비스의 특성과 기술환경에 맞추어 실효성 있는 대응 수단을 자율적으로 마련·시행하도록 유도하는 방향의 접근을 검토할 필요가 있다는 의견을 제시함.

<주요 메신저 사업자의 피싱 대응 사례>

메타의 메신저 피싱 대응 사례
메타는 사기 의심 계정에 대해 ‘경고 알림’ 기능을 도입(2026.3) ① (페이스북) 친구 신청을 한 사람이 프로필 국가와 현재 접속 국가가 다른 경우, 공통 친구가 별로 없는데 신청한 경우 등 ② (왓츠앱) 거짓 정보를 이용해 이용자에게 QR코드를 스캔하게 하거나 기기 연결 코드를 입력하도록 유도해서 사기꾼의 기기에 연결하는 것을 방지하기 위해 의심스러운 연결 요청이 감지될 경우 연결 요청이 어디에서 왔는지 알려주고 사기일 가능성 경고 ③ (인스타그램) 새로운 연락처와의 대화 내용에서 의심스러운 구인 광고와 같은 사기 패턴이 발견될 경우
카카오톡의 메신저 피싱 대응 사례
카카오는 자사의 ‘안티어뷰징 시스템’에 인공지능 및 머신러닝 등의 기술을 결합하여 사칭 사기·피싱 범죄 예방을 위한 ‘페이크 시그널’ 기능을 도입(2024.8) ① 카카오톡 프로필 정보와 계정 및 사용 이력 등을 분석하고 사칭 가능성이 높은 프로필을 자동으로 탐지함 ② 사칭 의심 프로필 이미지에는 경고 표시를 노출하고, 사칭 의심 계정을 친구 추가하거나 대화를 시도하면 경고 팝업 문구를 띄워 경고 알림을 전송하며, 해당 계정을 바로 차단하고 신고할 수 있는 경로를 안내

자료: 과학기술정보통신부

2) 한국인터넷기업협회: 신중검토

- 범죄 예방 목적으로 이용자의 해외 접속 국가를 표시할 경우 잦은 범죄 등으로 이미지가 좋지 않은 국가에서 접속 하는 이용자에 대한 부정적인 낙인으로 작용할 수 있고, 개인정보인 자신의 접속 국가를 구체적으로 노출되는 것에 거부감을 느끼는 이용자들이 많을 것으로 예상됨.
- 또한, 메신저서비스 제공자는 전문 수사기관이 아니므로 신고된 계정의 범죄 관련성 여부를 실질적으로 판단할 수 없어 지체없이 계정 정지 등 필요한 조치를 취하기 어렵고, 범죄 여부의 실질적 판단 없이 신고 접수만으로 계정 정지 등 조치가 이루어질 경우 허위·악의적 신고로 인한 이용자 피해가 발생할 우려도 있으므로 신중한 검토가 필요함.

문 의 처

02)6788-5225
